НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«На правах рукопису»
УДК 621.391

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра
зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Дослідження сценаріїв взаємодії телекомунікаційних мереж різних технологій на базі IMS»

Виконав (-ла):
студент (-ка) ІІ курсу, групи ТС-91мн
Мєщерінов Михайло Вячеславович _____

Керівник:
Доцент, кандидат технічних наук,
Гаттуров В.К. _____

Рецензент:
Доцент кафедри СК-3 ІСЗЗІ, кандидат технічних наук,
Мазор С.Ю. _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-науковою програмою

Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1 «Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Мєщерінову Михайлу Вячеславовичу

1. Тема дисертації «*Дослідження сценаріїв взаємодії телекомунікаційних мереж різних технологій на базі IMS*»,
науковий керівник дисертації Гаттуров Віктор Кавич доцент, кандидат технічних наук,
затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом дисертації _____

3. Об'єкт дослідження: конвергенція мереж ISDN та SIP за допомогою підсистеми IMS.

4. Предмет дослідження: алгоритми взаємодії мереж ЗКС №7 і SIP, і ефективність їх використання.

5. Перелік завдань, які потрібно розробити Проаналізувати принцип роботи мережі на базі IMS. Проаналізувати алгоритми взаємодії мережі на базі IMS з мережею ЗКС №7. Проаналізувати доцільність використання транспортних протоколів UDP та SCTP для трансляції трафіку. Експериментально дослідити доцільність використання протоколів UDP та SCTP.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу

Презентація 10 слайдів

7. Орієнтовний перелік публікацій

“ДОСЛІДЖЕННЯ СЦЕНАРІЇВ ВЗАЄМОДІЇ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗКС-7 З МЕРЕЖАМИ НАСТУПНОГО ПОКОЛІННЯ НА БАЗІ IMS.” / Михайло Вячеславович Мєщерінов / Збірник матеріалів Міжнародну науково-технічну конференцію студентів та аспірантів "Перспективи розвитку інформаційно-телекомунікаційних технологій та систем"– 2020.

“ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ МЕРЕЖІ NGN НА БАЗІ IMS ПРИ ПЕРЕДАЧІ ТРАФІКУ МЕРЕЖІ ЗКС №7 ЗА УМОВИ ВТРАТИ ПАКЕТІВ ПРИ ВИКОРИСТАННЯМ ПРОТОКЛІВ UDP ТА SCTP”/ Михайло Вячеславович Мєщерінов, Віктор Кавич Гаттуров / Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ». – 2021.

8. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз роботи мережі ЗКС №7	01.11.2019 – 01.03.2020	
2	Аналіз роботи мережі на базі IMS	02.03.2020 – 01.06.2020	
3	Аналіз транспортних протоколів мережі SIP	02.06.2020 – 01.09.2020	
4	Створення алгоритму моделі дослідження продуктивності протоколів UDP та SCTP	02.09.2020 – 01.12.2020	
5	Проведення дослідження, аналіз отриманих результатів, оформлення дипломної роботи	02.12.2020 – 18.04.2021	

Студент _____ Мєщерінов М.В.
(підпис) (ініціали, прізвище)

Керівник роботи _____ Гаттуров В.К.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Текстова частина роботи містить 73 сторінки, 25 рисунків.

Мета даної роботи полягає в аналізі алгоритму взаємодії мереж ЗКС №7 і SIP в телекомунікаційних мережах на базі IMS при використанні різних транспортних протоколів, і обґрунтування вибору одного з них.

В даній роботі розглядаються алгоритм трансляції трафіку мережі ЗКС №7 через мережу SIP при використанні протоколів UDP та SCTP. Проаналізовано продуктивність протоколів UDP та SCTP і експериментально визначено оптимальний протокол для процесу трансляції трафіку мережі ЗКС №7 через мережу SIP. На основі отриманих результатів надано рекомендації до використання протоколу UDP.

ЦИФРОВА МЕРЕЖА ISDN, ПРОТОКОЛ ISUP, ПРОТОКОЛ ВСТАНОВЛЕННЯ СЕАНСУ SIP, IMS, NGN, UDP, SCTP.

ABSTRACT

The purpose of this work is to analyze the algorithm of interaction of SS7 and SIP networks in telecommunication networks based on IMS using different transport protocols, and justify the choice of one of them.

In this paper, we consider the algorithm for translating traffic of the SS7 network over the SIP network using UDP and SCTP protocols. The performance of UDP and SCTP protocols was analyzed, and it was experimentally determined the optimal protocol for the process of broadcasting traffic of the SS7 network via the SIP network. Based on the obtained results, recommendations for the use of the UDP protocol are provided.

DIGITAL NETWORK ISDN, ISUP PROTOCOL, Session Initiation Protocol SIP, IMS, NGN, UDP, SCTP.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ISDN	Integrated Services Digital Network – цифрова мережа з інтеграцією служб.
ТМЗК	Телефонна мережа загального користування.
IP	Internet Protocol – міжмережевий протокол.
MTP	Message Transfer Part, підсистема передачі повідомлень.
ISUP	ISDN User Part, підсистема користувачів мережею ISDN.
SIP	Session Initiation Protocol – протокол встановлення сеансу.
VoIP	Voice over IP – телефоний зв’язок за протоколом IP.
TCAP	Transaction Capabilities Application Part, Підсистема застосування можливостей транзакцій
RTSP	Real Time Streaming Protocol – потоковий протокол реального часу.
SCCP	Signaling Connection and Control Part, підсистема підключення та управління сигналізацією
RTP	Real-time Transport Protocol, Транспортний протокол реального часу
TCP	Transmission Control Protocol, Протокол керування передачею
ЗКС №7	Мережа загальнокальної сигналізації №7.
MGCP	Media Gateway Control Protocol – протокол контролю медіашлюзів.
UDP	User Datagram Protocol, Протокол датаграм користувача
MSU	Message Signaling Unit, кадр передачі
MGC	Media Gateway Controler
ISUP	ISDN User Part – частина ЗКС №7.
MAP	Mobile Application Part, Підсистема мобільних додатків
INAP	Intelligent Network Application Part, Підсистема додатків інтелектуальних мереж

CAP	CAMEL (Customised Applications for Mobile networks Enhanced Logic) Application Part
LSSU	Link Status Signal Unit, кадр статусу передачі сигналу
SIF	Signaling Information Field, поле сигнальної інформації
IETF	Internet Engineering Task Force, відкрите міжнародне співтовариство проектувальників
IEEE	Institute of Electrical and Electronics Engineers, Інститут інженерів з електротехніки та електроніки
OSI	Базова еталонна модель взаємодії відкритих систем
RTP	Realtime Transport Protocol, транспортний протокол реального часу
CSCF	Call Session Control Function, функція керування викликами і сеансами
MGCF	Media Gateway Control Function, функція керування медіа шлюзами
UAC	User Agent Client, клієнт агента користувача
UAS	User Agent Server, сервером агента користувача
UA	User Agent, агент користувача
SCTP	Stream Control Transmission Protocol, протокол передачі з керуванням потоку
NGN	Next Generation Network, Мережа майбутнього покоління
GPL	GNU Public License

ВСТУП

В останні роки оператори мобільного зв’язку перебудовують свої мережі на мережі з комутацією каналів. При цьому однією з основних технологій, що використовується для побудови нових мереж майбутнього покоління є технологія мережі на підсистемі IMS. Велика кількість переваг даної технології зробили її привабливим варіантом для операторів мобільного зв’язку.

В той же час, в період бурхливого розвитку мереж з комутацією пакетів, потрібно не забувати про можливість взаємодії нових мереж наступного покоління з мережами минулих поколінь, в тому числі з мережею ЗКС №7, яка досі використовується, тому питання налагодження вдалої та продуктивної взаємодії мереж ЗКС №7 та NGN на базі IMS є актуальним.

Актуальність теми в тому, що для побудови сучасних мереж зв’язку використовують мереж NGN на базі IMS. В даній дипломній роботі розглядаються методи і алгоритми взаємодії мереж ЗКС №7 та SIP в межах архітектури IMS.

Об’єктом дослідження є конвергенція мереж ISDN та SIP за допомогою підсистеми IMS.

Предметом дослідження є алгоритми взаємодії мереж ЗКС №7 і SIP, і ефективність їх використання.

У першому розділі розглянуто мережу ЗКС №7, її архітектурі, формату та змісту її повідомлень.

Другий розділ присвячений загальним положенням мережі SIP, її архітектурі та послугам, які може надавати ця мережа. Також розглянуто протоколи UDP, TCP та SCTP як транспортні протоколи мережі SIP, підкресленні їх відмінності та доцільність їх використання в контексті взаємодії мереж ЗКС №7 і SIP.

У третьому розділі розглянуті алгоритми взаємодії мережі ЗКС №7 та мережі на основі протоколу SIP під час надання мультимедійних послуг та перетворення сигнальних повідомлень.

У четвертому розділі представлені результати експериментального дослідження показників продуктивності взаємодії мереж ЗКС №7 і SIP при виборі допоміжного транспортного протоколу між протоколами UDP та SCTP.

Таким чином, тема дипломної роботи присвячена алгоритмам взаємодії мереж ЗКС №7 та телекомунікаційних мереж на базі IMS є актуальною і сприяє подальшому розвитку телекомунікаційних мереж.

1 ТЕЛЕФОННА ЦИФРОВА МЕРЕЖА З ІНТЕГРАЦІЄЮ ПОСЛУГ

1.1 Телефонні мережі загального користування

Телефонна мережа загального користування, ТМЗК (англ. PSTN, Public Switched Telephone Network) - це мережа, яка являє собою сукупність пристроїв і споруд, що забезпечують телефонний зв'язок на деякій території для доступу до якої використовуються звичайні провідні телефонні апарати. [5]

Передача сигналів (в тому числі і настройка з'єднання) і сама розмова здійснюється через одну і ту ж універсальну лінію зв'язку від джерела до адресата. Цей процес займає канали зв'язку всіх задіяних при з'єднанні пристроїв.

В телефонії сигналізацією називають передачу керуючої інформації для встановлення / роз'єднання з'єднань «точка-точка». Розроблена з метою підвищення ефективності функціонування телефонних мереж, система загально канальної сигналізації №7 (Signaling System 7, SS7) грає важливу роль в процесі конвергенції мереж. Вона була створена для передачі керуючих сигналів по мережі з комутацією пакетів окремо від основної мережі (out-of-band signaling). Раніше в телефонних мережах передача мови і сигналів управління відбувалася по одному каналу (inband signaling). З ростом обсягу і видів інформації, що передається, появою нових послуг таке використання каналів стало неефективним. До того ж розроблені для національних мереж аналогові системи сигналізації приводили до труднощів при взаємодії з іншими мережами. [5]

Впровадження ЗКС №7 дає операторам телефонних мереж можливість гнучко формувати нові послуги на базі вже існуючого обладнання. Система сигналізації забезпечує високу швидкість встановлення з'єднання і передачі даних (без втрат і дублювання), перемикання трафіку на альтернативні маршрути в разі відмов, зручну для обробки структуру повідомлень, трансляцію номерів абонентів. До переваг ЗКС №7 відносять також більшу економічність (на комутаційної станції потрібно в кілька разів менше

обладнання), високу продуктивність (обслуговування одним каналом сигналізації тисяч викликів), підвищену надійність (завдяки альтернативної маршрутизації сигналів і резервування каналів).[8]

В даний час ЗКС №7 становить сигнальну інфраструктуру операторів місцевого, міжміського, міжнародного та бездротового зв'язку. Ця пакетна мережа передачі даних стала важливою частиною телефонних і стільникових мереж. У мережах ТМЗК мережі ЗКС №7 працюють у багатьох країнах вже не один десяток років. Сфера їх застосування поширюється і на широкосмугові мережі, і на додатки комп'ютерної телефонії. Загальноканальна сигналізація ЗКС №7 стала важливим елементом великих телекомунікаційних мереж. [8]

1.2 Опис мережі ЗКС №7 та її підсистем

Загальноканальна сигналізація №7 – це стек протоколів, що описують способи комунікації між телефонними розподільниками (комутаторами) у відкритих телефонних мережах. Використовується телефонними компаніями для міжстанційної сигналізації. У минулому, використовувався односмуговий зв’язок - був один загальний канал для передачі корисного трафіку та повідомлень сигналізації телефонних дзвінків. Даний метод не був ефектним і згодом був замінений на багатосмуговий. [6]

Ще не так давно, всі телефонні з'єднання здійснювались різноманітними техніками, заснованими на внутрішньосмуговій загальноканальній сигналізації.

Мережа, що використовує поза смугову загальноканальну сигналізацію, являє собою сукупність двох мереж в одній:

- Мережа з комутацією каналів, яка забезпечує передачу голосу і даних. Здійснює фізичний канал між відправником і отримувачем.
- Мережа сигналізації, забезпечує передачу службової інформації, що управляє викликом. [6]

ЗКС №7 є взаємозамінним набором мережевих елементів, які використовуються для обміну повідомленнями для підтримки

телекомунікаційних функцій. Протокол ЗКС №7 розроблений з метою просування цих можливостей і обслуговування мережі, на якій вони надаються.

Стек протоколів ЗКС №7 відповідає моделі OSI, але має тільки чотири рівні. Рівні збігаються з рівнями OSI 1 (фізичний), 2 (канальний) і 3 (мережевий). Рівень 4 ЗКС №7 відповідає рівню 7 OSI. Рівні називаються MTP (англ. Message Transfer Part) 1, MTP 2 і MTP 3. Рівень 4 ЗКС №7 містить кілька різних користувацьких рівнів, наприклад Telephone User Part (TUP), ISDN User Part (ISUP), Transaction Capabilities Application Part (TCAP) і Signaling Connection and Control Part (SCCP). [6] Загальний вигляд архітектури ЗКС №7 показано на рисунку 1.1.

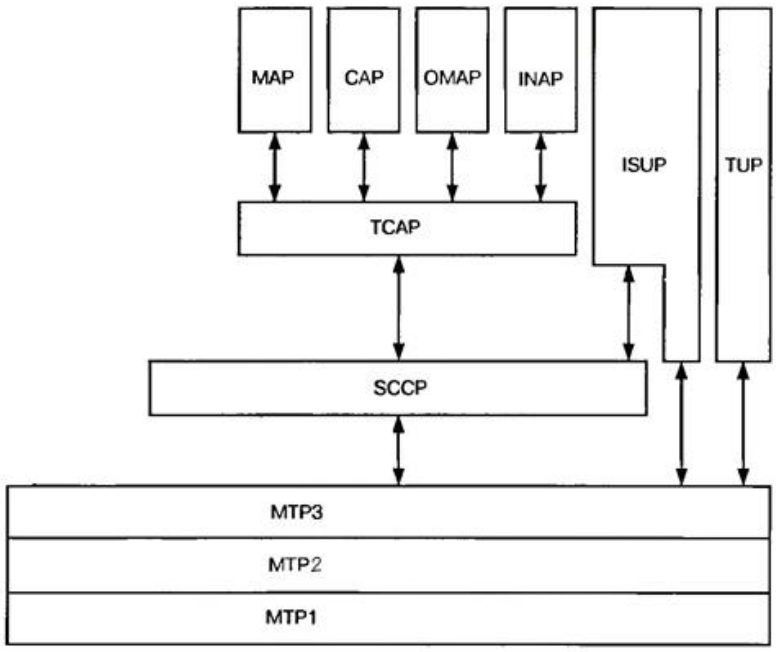


Рисунок 1.1 - Рівні мережі ЗКС7

Message Transfer Part – Підсистема передачі повідомлень. Підсистема MTP поділяється на три логічні рівні, кожен з яких виконує своє окреме завдання.

MTP1. На даному рівні виконуються функції електронно-оптичного перетворення, забезпечення необхідної потужності сигналу передачі. MTP1 сумісний з різними інтерфейсами (E1, T1).

На цьому рівні формується 3 види кадрів.

MSU (Message Signaling Unit) - кадр передачі, який використовується для передачі сигнальних повідомлень (для організації, розриву з'єднань і т.д.). [6]

Будова кадру MSU показана на рисунку 1.2.

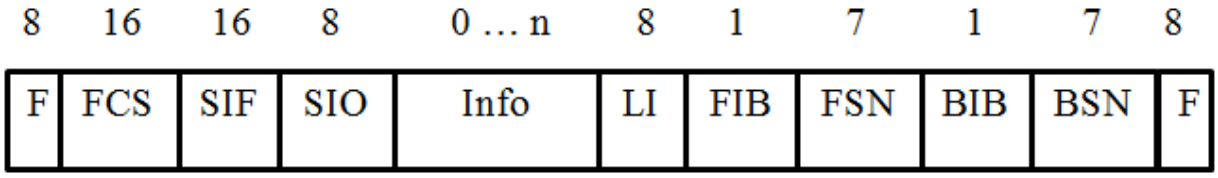


Рисунок 1.2 - Будова кадру MSU

Цифри - кількість біт кожного поля. Призначення всіх полів буде описано далі.

LSSU (Link Status Signal Unit) - кадр передачі, який несе інформацію про статус сигнальних повідомлень, про стан з'єднання сигналізації. [6]

Будова кадру LSSU показана на рисунку 1.3.

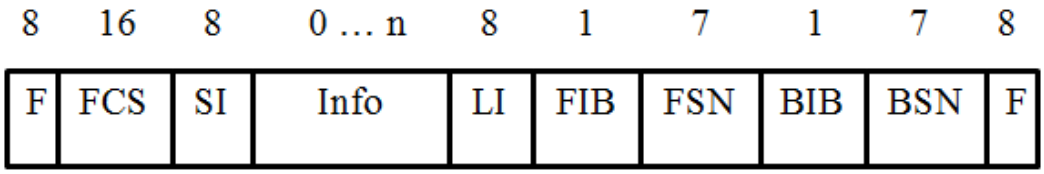


Рисунок 1.3 - Будова кадру LSSU

Як бачимо, різниця між ними в відсутності частини SIO, про яку буде згадано нижче.

FISU (Fill In Signaling Unit) – даний тип кадру не несе інформації і називається «порожнім». Застосовується в разі односпрямованої передачі сигнальних повідомлень приймають вузлом для сигналізації передавальному вузлу про наявність помилок і організації повторної передачі.

MTP2. Виконує наступні функції: кадрова синхронізація, перевірка помилок при передачі одного кадру, узгодження швидкості передачі, організація повторної передачі кадрів, в яких виявлені помилки. [6]

На цьому рівні формується 3 види кадрів.

- MSU (Message Signaling Unit) - кадр передачі, який використовується для передачі сигнальних повідомлень (для організації, розриву з'єднань і т.д.).
- LSSU (Link Status Signal Unit) - кадр передачі, який несе інформацію про статус сигнальних повідомлень, про стан з'єднання сигналізації.
- FISU (Fill In Signaling Unit) - даний тип кадру не несе інформації і називається «порожнім». Застосовується в разі односпрямованої передачі сигнальних повідомлень приймальним вузлом для сигналізації передавальному вузлу про наявність помилок і організації повторної передачі. [6]

МТР3. Функції даного рівня збігаються з функціями мережевого рівня моделі OSI. Виконує адресацію в мережі ЗКС №7, маршрутизацію.

На МТР3 формуються поля SIO, SIF і SI. [6]

Будова полів SIO та SIF показана на рисунку 1.4.

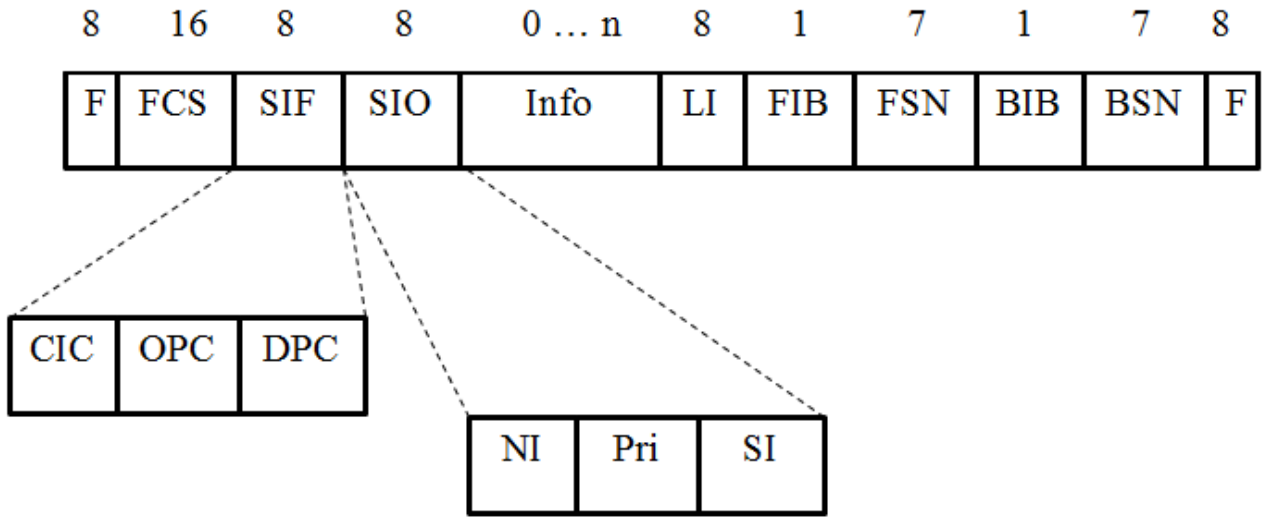


Рисунок 1.4 - Формування полів SIO та SIF

Поле SIF (Signaling Information Field) застосовується для вказівки ID коду сигнального вузла, при цьому, вказується код вузла, який передає повідомлення

OPC (Originating Point Code), як і код вузла, якому призначено дане повідомлення DPC (Destination Point Code).

Поле CIC (Circuit Identity Code) застосовується для вказівки тимчасового інтервалу (time-slot), який застосовується для передачі сигнальних повідомлень і знаходиться в одному з потоків E1, T1. [6]

Поле SIO (Service Information Octet) застосовується для ідентифікації типу послуги. NI (Network Indicator) - індикатор живлення, служить для вказівки типу мережі (національна або міжнародна мережа). Pri (Priority) - це поле, зазвичай, є резервом, в окремих випадках може застосовуватися для вказівки пріоритету. SI (Service Indicator) - вказує до якого типу послуг відноситься сигнальне повідомлення, яке знаходиться в інформаційному полі. [6]

На третьому рівні формуються сигнальні сполуки між вузлами. На рисунку 1.5 показано сигнальні сполуки між вузлами.

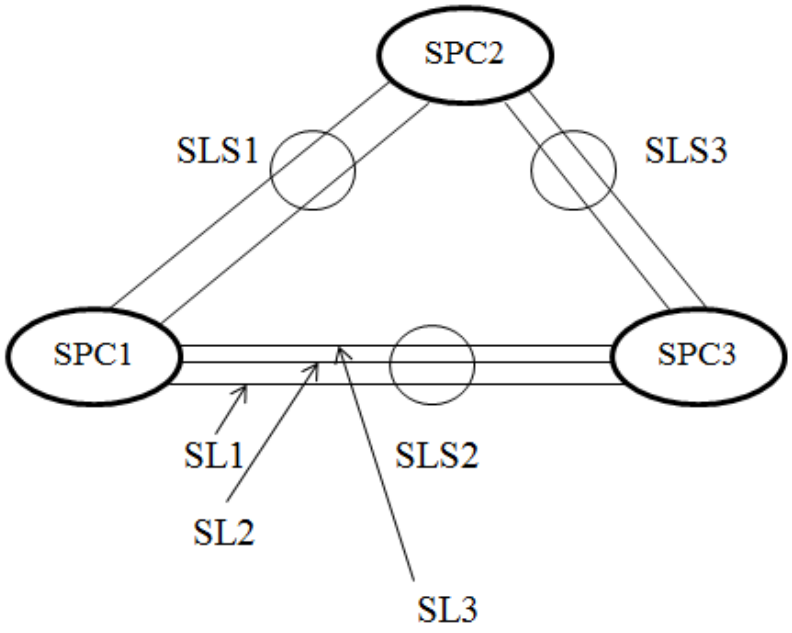


Рисунок 1.5 - Сигнальні сполуки між вузлами.

SL (Signaling Link) – це з’єднання між двома вузлами, через які відбувається обмін сигнальними повідомленнями. Як правило, число SL більше 2-х. Два SL, що зв’язують два вузла сигналізації, зазвичай входять в набір

сигнальних ліній SLS (Signaling Link Set). Набір SLS може містити 2, 3 і більше SL, в залежності від ємності сполучної лінії між АТС. [6]

У мережі ЗКС №7 розрізняють три типи сигнальних вузлів:

- SSP (Signaling Switching Point) – вузол, що виконує комутацію вузлів.
- SCP (Signaling Control Point) – контролює роботу SSP, містить базу даних, керуючи тим самим доступом до послуг, які надає SSP.
- STP (Signaling Transfer Point) – вузол, виконуючий функції маршрутизації сигнальних повідомлень.

Telephony User Part (TUP). Даний рівень містить набір протоколів, що надає можливість застосування ЗКС7 в аналогової мережі стаціонарної телефонії, адаптований до системи сигналізації з поєднаним каналом, що застосовується в аналогової абонентської лінії. В даний час не використовується.

ISDN User Part (ISUP). Набір протоколів, що дозволяє застосування ЗКС7 в мережах ISDN. Підтримує принцип роботи всіх інтерфейсів ISDN, визначає алгоритм формування з'єднань. [6]

Signaling Connection Control Part (SCCP). Система управління з'єднанням каналів сигналізації. Виконує функції контролю за з'єднаннями в мережі ЗКС7. Дозволяє організувати 4 види передачі даних. Кожен вид характеризується класом від 0 до 3.

- Class 0. Формування з'єднань без узгодження між терміналами.
- Class 1. Формування з'єднання з урахуванням номера послідовності при передачі. Не орієнтоване на з'єднання.
- Class 2. Формування з'єднання з попереднім узгодженням, після відбувається передача.
- Class 3. Формування з'єднання з попереднім узгодженням, після якого відбувається передача даних з контролем швидкості передачі. [6]

Transanction Capability Application Part (TCAP). Забезпечує функції обробки даних для роботи обладнання з віддаленим доступом. TCAP застосовується для забезпечення роумінгу між мережами. У цьому випадку

використовується послуга «глобального перекладача», яка переводить код сигнального вузла (SIF) в формат телефонного номера. [6]

Підсистема TCAP взаємодіє з наступними підрівнями:

- Mobile Application Part (MAP). Набір протоколів, що дозволяє застосовувати ЗКС7 в мобільній мережі. В цьому випадку, дані протоколи підтримують всі інтерфейси мобільної мережі, визначають принцип hand-over, принципи формування з'єднань.
- Inteligent Network Application Part (INAP). Даний набір протоколів служить для застосування ЗКС7 в інтелектуальних мережах зв'язку (IN). Визначає принцип формування з'єднань в IN. При цьому, можливо застосування автентифікації, як методу перевірки дійсності абонента.
- CAP (CAMEL Application Part). CAP це набір стандартів реалізації інтелектуальних послуг усіх інших послуг. Основна відмінність від INAP, яке за призначенням призначене для цих же цілей - це незалежність від виробника обладнання та, як наслідок, можливість використання послуг при охороні в господарських мережах. [7]

Основний принцип інтелектуальних мереж полягає в перегляді логіки обробки виклику з комутатором, який у цьому випадку відповідає лише за комутацію визова і називається Service Switching Point (SSP), на зовнішньому контрольованому вузлі – Service Control Point (SCP). Завдяки такому розділенню з'являється можливість реалізувати нові послуги (а також модифікувати існуючі) без тривалих і дорогостійких змін у програмному забезпеченні комутаторів. CAMEL або CAP дозволяє забезпечити повний пакет інтелектуальних додаткових послуг (насамперед роумінг) своїм абонентам (включаючи абонентів передоплати) не тільки в домашній мережі, але в роумінгу в мережах, що підтримують стандарт CAMEL, за рахунок можливості контролю рахунків і тарифікації в домашній мережі в режимі реального часу. [7]

OMAP (Operation and Maintenance Application Part). Підсистема аплікацій експлуатації й технічного обслуговування.

Підсумовуючи, стек протоколів ЗКС №7 має чотирьох рівневу будову. Перші три рівні мережі ЗКС7 називаються MTP1, MTP2 та MTP3. Рівень 4 мережі ЗКС7 містить декілька різних за призначенням для користувача рівнів, основні з яких ISUP, TCAP та SCCP. Рівні MTP описують транспортні протоколи, включаючи мережеві інтерфейси, обмін даними, обробка повідомлень і маршрутизація їх на верхній рівень. SCCP - це підрівень з інших протоколів 4 рівня, і разом з MTP3 може бути названий як Network Service Part (NSP). NSP забезпечує адресацію і маршрутизацію повідомлень без встановлення з'єднання (UDT) і сервіс управління для інших частин 4 рівня. ISUP - це ключовий протокол, що надає канально-орієнтований протокол для установки, підключення і завершення з'єднання при дзвінку. TCAP використовується для створення запитів до бази даних і використовується при розширеній функціональності мережі або як сполучний протокол з інтелектуальними мережами (INAP), мобільними службами (MAP) і т.д.

1.3 Структура підсистеми ISUP

ISUP (ISDN User Part) - підсистема користувача цифрової мережі інтегрального обслуговування (ISDN). Є частиною протоколу ЗКС №7.

Припускає перенесення сигнальної інформації мережі ISDN через інфраструктуру телефонної мережі загального користування (ТМЗК). Для перенесення інформації підсистема ISUP використовує послуги, що надаються підсистемою передачі повідомлень (MTP - message transfer part). На рисунку 1.6 показано місце технології ISUP в мережі ЗКС №7. [13]

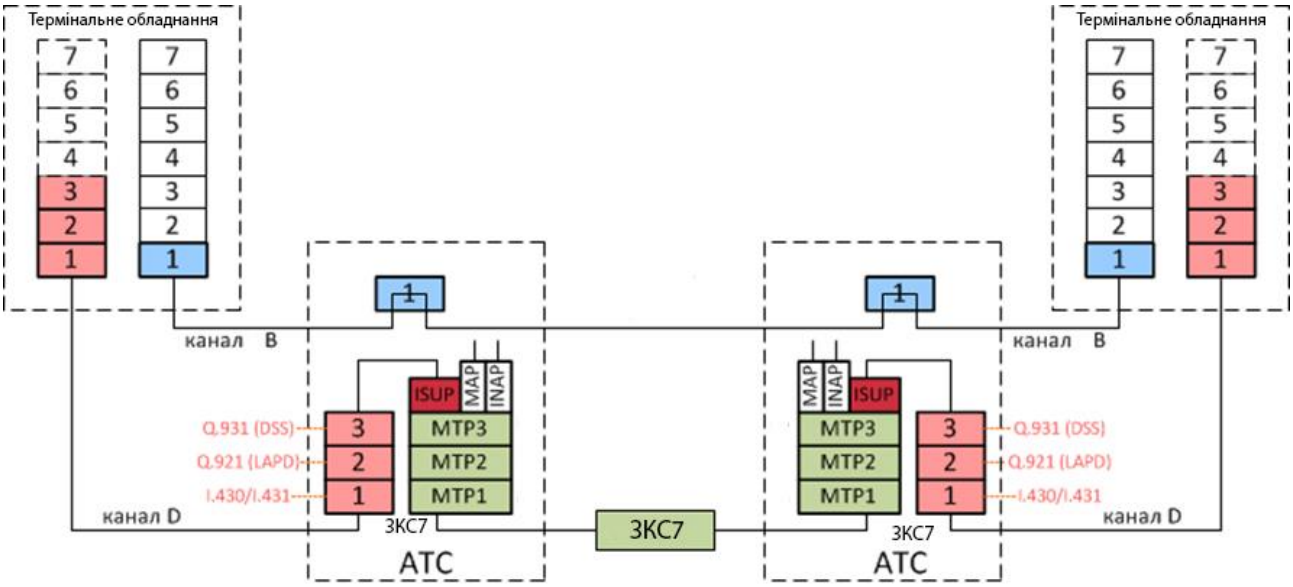


Рисунок 1.6 - Місце технології ISUP в мережі ЗКС №7

В ЗКС №7 сигнальна інформація організовується у вигляді пакетів, які передаються між пунктами сигналізації у вигляді повідомлень змінної довжини (сигнальні одиниці) трьох типів: MSU (Message Signalling Unit), LSSU (Link Status Signal Unit), FISU (Fill-in Signal Unit). [13]

Підсистеми ISUP для обміну сигнальною інформацією між собою використовують тільки MSU (значущі сигнальні одиниці). Структура поля MSU показано на рисунку 1.7. [13]

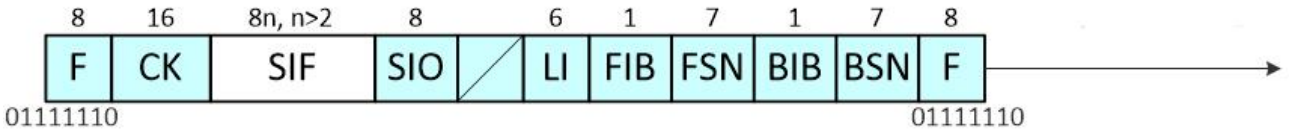


Рисунок 1.7 - Структура повідомлення MSU

F (Flag) - прапор - відзначає початок і кінець кожної MSU в безперервно надходячому потоці унікальною 8-бітової послідовністю. [13]

CK (Check Bits) - перевірочні біти - необхідні для відстеження виникаючих помилок в прийнятій MSU. [13]

SIO (Service Information Octet) - байт службової інформації - визначає, який саме підсистемі належить дана MSU (в нашому випадку це ISUP) і вид мережі (міжнародна, національна, місцева і т.п.). [13]

LI (Length Indicator) - індикатор довжини - визначає тип сигнальної одиниці (напр. MSU). [13]

FSN (Forward Sequence Number) і BSN (Backward Sequence Number) - прямий і зворотний порядкові номери MSU - це двійкові числа в циклічно повторюється послідовності від 0 до 127, необхідні для підтвердження прийому послідовності передачі MSU. [13]

FIB (Forward Indicator Bit) і BIB (Backward Indicator Bit) - прямий і зворотний біт-індикатори - використовуються в базовому методі виправлення помилок. [13]

SIF (Signaling Information Field) - поле сигнальної інформації - призначене для передачі корисної інформації по мережі ЗКС №7 (в т.ч. ISUP). MTP не розпізнає вміст SIF, крім етикетки маршрутизації, тобто прозоро передає інформацію всередині SIF. [13]

Всі повідомлення ISUP мають загальний формат (рисунок 1.8) і переносяться в полі сигнальної інформації (SIF).

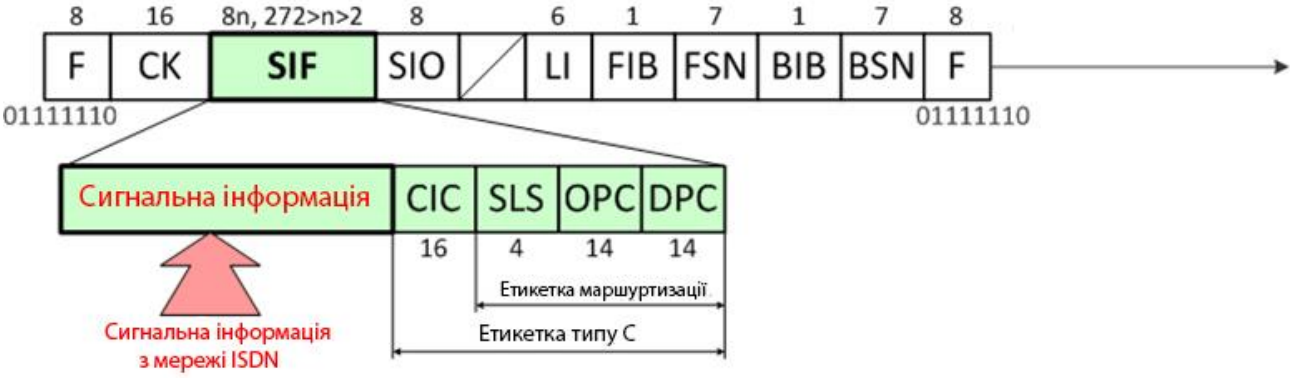


Рисунок 1.8. Структура поля SIF

Поле сигнальної інформації містить етикетку маршрутизації, код ідентифікації каналу, коду типу повідомлення і параметри. Параметри діляться на обов'язкові (присутні в повідомленні завжди) і необов'язкові. [13]

Етикетка маршрутизації

Поля DPC, OPC та SLS разом утворюють етикетку маршрутизації.

Для відправки сигнальної одиниці необхідно вказати, куди її треба передати. Код пункту призначення (DPC, destination point code) довжиною 14 бітів вказує номер пункту сигналізації, якій адресовано повідомлення. [11]

У деяких випадках необхідна інформація про відправника сигнальної одиниці. Код вихідного пункту (OPC, originating point code) визначає номер пункту сигналізації відправника. Довжина поля OPC складає 14 бітів. [11]

У разі, коли необхідно рівномірний розподіл навантаження між сигнальними ланками, використовується поле вибору сигнальної ланки (SLS, signaling link selection), довжина якого дорівнює 4 біта. [11]

Код ідентифікації каналу (CIC, circuit identity code). Має довжину два байта і вказує номер розмовного каналу між двома станціями, до якого належить передане повідомлення. Так, якщо використовується цифровий тракт 2048 кбіт/с, то п'ять молодших бітів CIC кодують в двійковому вигляді номер мовного тимчасового інтервалу, а залишені 7 біт використовуються для вказівки до якого ІКМ потоку належить цей мовний інтервал. [11]

Код типу повідомлення. Ідентифікує конкретне повідомлення ISUP.

Обов'язкова фіксована частина повідомлення (mandatory fixed part). Обов'язкові параметри фіксованої довжини, що утворюють обов'язкову фіксовану частину повідомлення, повинні бути присутніми в повідомленні завжди. Позиція, довжина і порядок проходження таких параметрів фіксовані для кожного типу повідомлення, тому ідентифікатори і довжини цих параметрів в повідомленні не вказуються. [14]

Обов'язкова змінна частина повідомлення (mandatory variable part). Обов'язкові параметри змінної довжини, що утворюють обов'язкову змінну частину повідомлення, повинні бути присутніми в повідомленні завжди. Оскільки довжина повідомлення заздалегідь невідома, то для обчислення початку наступного параметра використовують покажчик, який кодується одним байтом, і індикатор довжини параметра. Тип повідомлення однозначно

визначає порядок проходження і ідентифікатори всіх обов'язкових параметрів змінної довжини. [14]

Необов'язкові параметри (optional part). Це параметри, які можуть як бути присутніми, так і не бути присутнім в даному типі повідомлення. Довжина їх може бути фіксованою або змінною. Крім того, необов'язкові параметри можуть бути передані в будь-якому порядку. Кожен необов'язковий параметр містить своє ім'я (19 байт) і ідентифікатор довжини (1 байт), за якими слід саме вміст параметра. [14]

Покажчик (pointer). Застосовується для того, щоб визначити початок необов'язкової частини повідомлення. Якщо тип повідомлення має на увазі відсутність необов'язкової частини, то і покажчик відсутній. Якщо ж тип повідомлення передбачає, що необов'язкова частина можлива, поле покажчика обов'язково присутнє, а його значення містить кількість байт до початку необов'язкової частини, або дорівнює нулю, якщо необов'язкової частини в цьому повідомленні немає. У разі, коли в повідомленні немає обов'язкових параметрів змінної довжини, але можливі необов'язкові параметри, покажчик на необов'язкові параметри теж присутній. [14]

Кінець необов'язкових параметрів (end of optional parameters). Якщо в повідомленні присутні необов'язкові параметри, то завершує повідомлення байт «кінець необов'язкових параметрів» (що містить одні нулі). Якщо необов'язкові параметри відсутні, то цей байт теж відсутній. [14]

Отже, повідомлення підсистеми ISUP переносяться за допомогою типу повідомлення MSU, яке має багато полів, кожне з яких переносить свою важливу для з’єднання інформацію. Саме повідомлення підсистеми ISUP займає там лише невелике поле SIF, розмір якого не є постійним.

1.4 Процес обслуговування базового виклику

Процедуру встановлення та завершення з'єднання між вихідною точкою А та вхідною точкою В кінцевими станціями через транзитну станцію із використанням повідомлень ISUP показано на рисунку 1.9.

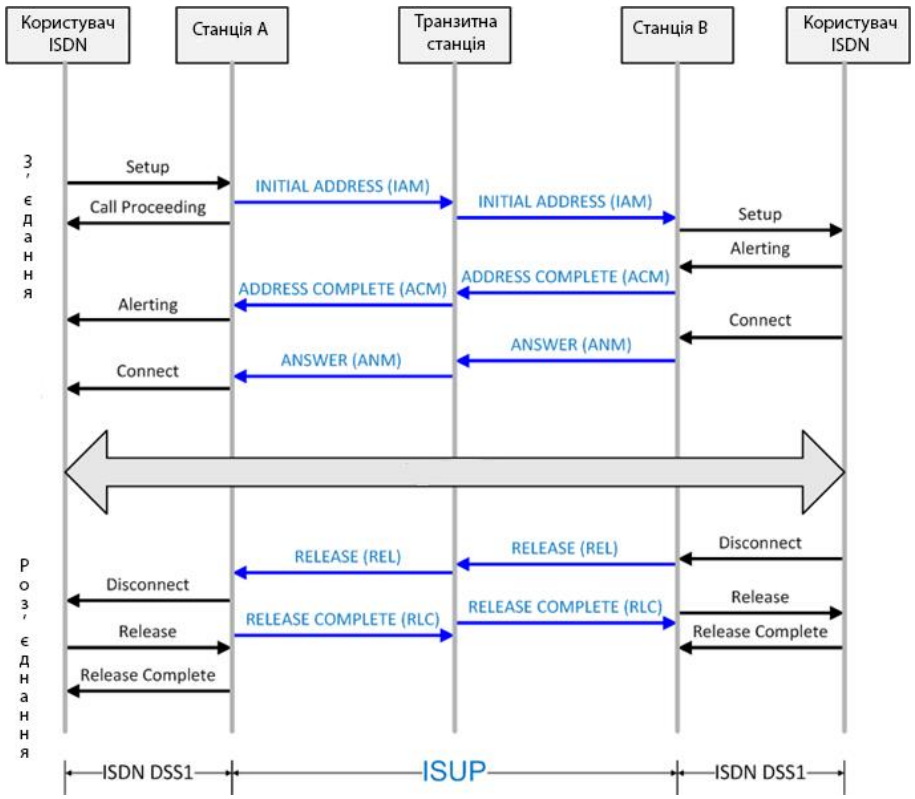


Рисунок 1.9 - Алгоритм базового з’єднання через підсистему ISUP

На ділянці від кінцевого терміналу абонента ISDN до АТС використовується протокол сигналізації DSS-1 (Digital subscriber signaling), на міжстанційній ділянці протокол ЗКС №7 (в даному випадку – підсистема ISUP).

Коли користувач ініціює ISDN-виклик (наприклад, взявши слухавку телефонного апарату), тоді вихідне термінальне обладнання абонента А надсилає повідомлення SETUP по D-каналу до кінцевої станції А.

При прийомі запиту встановлення з'єднання від абонента вихідна АТС А аналізує інформацію про маршрут і формує початкове адресне повідомлення IAM. Повідомлення IAM передає адресну інформацію, а також інформацію, що відноситься до встановлення з'єднання.

Аналіз номера абонента В, що викликається, дозволяє вихідній АТС А визначити напрямок маршрутизації виклику. Виклик направляється до транзитної станції, яка також виконує функції транзитного пункту сигналізації STP, в результаті чого відповідний розмовний тракт підключається в зворотному напрямку до абоненту для прослуховування акустичних сигналів.

Для встановлення з'єднання можливе використання двох режимів передачі адресної інформації: блоковий режим і режим з перекриттям.

При використанні блокового режиму вся адресна інформація, необхідна для маршрутизації виклику до абоненту, включаються в повідомлення IAM. У режимі «з перекриттям» (overlap), повідомлення IAM надсилається тоді, коли прийняті цифри, необхідні тільки для маршрутизації до транзитної АТС, а цифри, що залишилися, передаються через мережу в наступних адресних повідомленнях (SAM).

Транзитна АТС приймає повідомлення IAM і аналізує записану в ньому інформацію. Аналіз цифр номера абонента, що викликається на транзитній АТС, визначає подальший маршрут до вхідної АТС В. Транзитна станція формує нове повідомлення IAM, передає його до АТС В і підключає розмовний тракт в обох напрямках.

При надходженні повідомлення IAM на вхідну АТС В, проводиться аналіз номера абонента, що викликається, і того, чи потрібно додаткова інформація від вихідної АТС А перед підключенням до абонента, якому телефонують. Якщо потрібна додаткова інформація, то на вихідну АТС А направляється повідомлення запиту додаткової інформації INR методом з кінця в кінець, в якому міститься цей запит. Зауважимо, що транзитній АТС не потрібно аналізувати це повідомлення, так як для цього повідомлення має місце прозора передача. Вихідна АТС А надає відповідну інформацію, посилаючи у відповідь повідомлення Інформація (INF).

Після прийому необхідної інформації абонент В вхідної АТС В інформується про вхідний дзвінок, а від вхідної АТС В до транзитної АТС надсилається повідомлення Адреса достатня (ACM). Повідомлення ACM про

прийом повної адреси потім передається до вихідної АТС А. Прийом повідомлення про прийняття повної адреси на будь-якій станції, що приймає участь у встановленні з'єднання, вказує на успішну маршрутизацію виклику до абонента АТС В і дозволяє видалити з пам'яті інформацію, пов'язану з з'єднанням.

Коли абонент відповідає на виклик (передає повідомлення connect), вхідна АТС В підключає розмовний тракт і передає повідомлення Відповідь (ANM) на транзитну АТС, яка, в свою чергу, пересилає повідомлення ANM на вихідну АТС А. При прийомі повідомлення відповіді вихідна АТС А підключає розмовний тракт в прямому напрямку. Таким чином встановлюється з'єднання телефонуючого і викликаного абонентів, починається тарифікація виклику і здійснюється розмова або передача даних.

У підсистемі ISUP використовується метод одностороннього відбою. Розірвання з'єднання може бути ініційовано будь-яким його учасником, при цьому сама процедура в будь-якому випадку одна і та ж. Викликаний абонент перший направляє сигнал роз’єднання Disconnect до вхідної АТС В.

Вхідна АТС В розриває розмовний тракт в обох напрямках і передає повідомлення Роз'єднання (REL) транзитній станції. Транзитна станція, отримавши від АТС В повідомлення REL, також розриває розмовний тракт в обох напрямках, передає повідомлення REL до вихідної АТС А і повідомлення Підтвердження роз'єднання (RLC) - назад до АТС В. Як тільки повідомлення REL досягає АТС А, та одразу ж розриває розмовний тракт в обох напрямках і передає викликаній стороні повідомлення Disconnect протоколу DSS-1 та повідомлення RLC до транзитної станції.

В цілому, процес утворення з’єднання має чітку послідовну структуру, свій набір повідомлень та відповідей, та набором інструкцій для реагування на ті чи інші повідомлення, або їх відсутність.

1.5 Висновки до розділу 1

Мережа ТМЗК, як і підсистема ISUP – приклад мережі з комутацією каналів, де голосовий зв’язок йде безперервним потоком даних. Мережа NGN на базі IMS є прикладом мережі з комутацією пакетів, де голосовий зв’язок йде розділеним на масиви даних. Головною задачею для забезпечення голосового зв’язку мережі з комутацією каналів та мережі з комутацією пакетів є забезпечення гарантованої, своєчасної та послідовної доставки даних. Принцип роботи мережі NGN на базі IMS, та методи досягнення зазначених вимог, розглянуті в наступних розділах

2 МЕРЕЖА NGN НА БАЗІ IMS

2.1 Архітектура підсистеми IMS

Мультимедійна IP підсистема IMS проектувалася в рамках мережі 3G, яка повністю базується на IP. Основним її протоколом є SIP, що дозволяє встановлювати однорангові сесії між абонентами і використовувати IMS лише як систему, яка надає сервісні функції з безпеки, авторизації, доступу до послуг і т.д. Функція управління шлюзами, як і сам медіашлюзи тут лише засіб для зв'язку абонентів 3G з абонентами фіксованих мереж. Причому маються на увазі лише ТМЗК, які функціонують на протоколі ЗКС №7. [17]

Архітектура мережі на базі IMS включає в себе блок інтерфейсів, SIP-проксі серверів і звичайних серверів, а також медіа шлюзів (для приєднання до мереж з протоколом, відмінним від IP). Сервісна архітектура представляє собою набір логічних функцій, які можна розділити на три рівні (рисунок 2.1) [17]:

- рівень транспорту і абонентських приладів;
- рівень керування сеансами;
- рівень додатків.

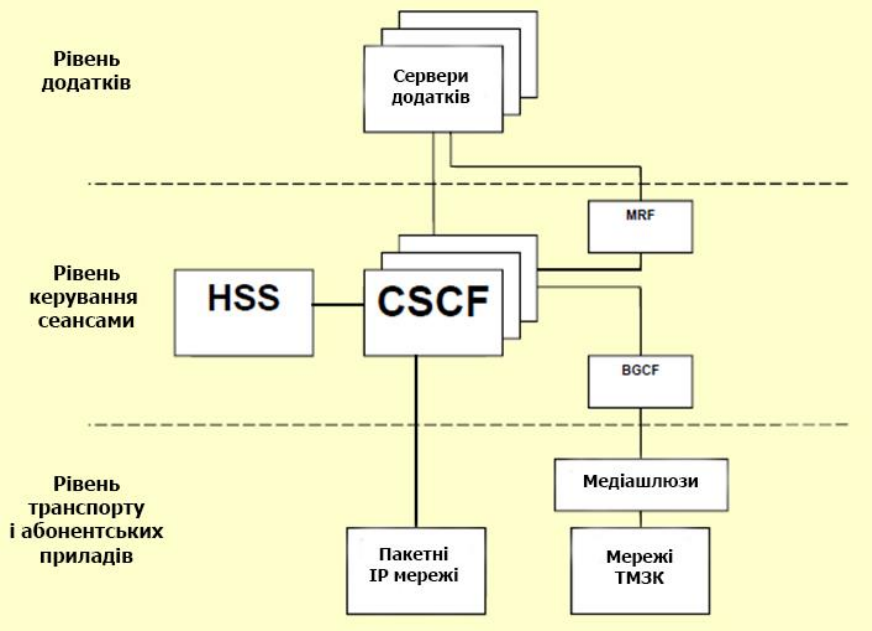


Рисунок 2.1 Архітектура мережі IMS

На рівні транспорту і абонентських пристроїв ініціюється і термінується сигналізація SIP, необхідна дня встановлення сеансів і надання базових послуг, таких як перетворення мовлення з аналогової або цифрової форми в IP-пакети з використанням протоколу RTP (Realtime Transport Protocol). На цьому рівні функціонують медіа, шлюзи, перетворюючи базові потоки VoIP в телефонний формат TDM. [17]

На другому рівні реалізується функція керування викликами і сеансами CSCF (Call Session Control Function), яка реєструє абонентські пристрої і направляє сигнальні повідомлення протоколу SIP до відповідних серверів додатків. Функція CSCF зв'язана з рівнем транспорту і доступу для забезпечення якості обслуговування за всіма сервісами. Рівень керування викликами і сеансами включає в себе сервер абонентських даних HSS (Home Subscriber Server), де централізовано зберігаються унікальні сервісні профілі всіх абонентів. На рівні керування викликами і сеансами також розташовується функція керування медіа шлюзами MGCF (Media Gateway Control Function), яка забезпечує взаємодію сигналізації SIP з сигналізацією інших медіа-шлюзів (наприклад, H.248). Функція MGCF управляє розподіленням сеансів по множині медіа шлюзів; для медіа серверів це виконується функцією MSFC (Media Server Function Control). Функція CSCF в IMS розділена на три під функції [17]:

- Proxy CSCF – через неї в систему IMS поступає весь трафік користувачів;
- I-CSCF – Interrogating (запитуючий) CSCF. Представляє собою точку з'єднання з домашньої мережею I-CSCF звертається до HSS, щоб знайти S-CSCF для конкретного абонента;
- S-CSCF – Serving (обслуговуючий) CSCF. Обробляє всі SIP – повідомлення, якими обмінюються кінцеві пристрої.

Рівень послуг складається з серверів додатків і контент-серверів для надання абонентам додаткових послуг. Базові засоби надання послуг, як це визначено стандартом IMS, реалізовані в якості послуг на сервері SIP –

додатка. Сервери додатків забезпечують обслуговування кінцевих користувачів. Архітектура IMS і сигналізація SIP забезпечують достатню гнучкість для підтримки різноманітних телефонних і інших серверів додатків. Так, наприклад, розроблені стандарти SIP для послуг телефонії і послуг IMS. [17]

SIP є основним протоколом мережі NGN на базі IMS, та відіграє свою роль на кожному з трьох рівнів архітектури IMS. [17]

2.2 Структура мережі на основі протоколу SIP, роль SIP в мережі на основі IMS

SIP (Session Initiation Protocol - протокол встановлення сеансу) - стандарт на спосіб встановлення і завершення користувацького інтернет-сеансу, що включає обмін мультимедійним вмістом (відео- і аудіоконференція, миттєві повідомлення, онлайн-ігри). [12]

У моделі взаємодії відкритих систем SIP є мережевим протоколом прикладного рівня. Розробкою займалася організація IETF. У листопаді 2000 року SIP був затверджений як сигнальний протокол проекту 3GPP і основний протокол архітектури IMS. Поряд с іншим поширеним протоколом H.323, SIP - один з протоколів, що лежать в основі VoIP. [12]

В основу протоколу закладалися такі принципи:

- Простота: включає в себе тільки шість методів (функцій)
- Незалежність від транспортного рівня, може використовувати UDP, TCP, SCTP і т. Д.
- Персональна мобільність користувачів. Користувачі можуть переміщатися в межах мережі без обмежень. Це досягається шляхом присвоєння користувачу унікального ідентифікатора. При цьому набір послуг, що надаються залишається незмінним. Про свої переміщення користувач повідомляє за допомогою повідомлення REGICTER. [12]

- Масштабованість мережі. Структура мережі на базі протоколу SIP дозволяє легко її розширювати і збільшувати число елементів.
- Можливість розширення протоколу. Протокол характеризується можливістю доповнювати його новими функціями при появі нових послуг.
- Інтеграція в стек існуючих протоколів Інтернет. Протокол SIP є частиною глобальної архітектури мультимедіа, розробленої комітетом IETF. Крім SIP, ця архітектура включає в себе протоколи RSVP (протокол), RTP, RTSP, SDP. [12]
- Взаємодія з іншими протоколами сигналізації. Протокол SIP може бути використаний спільно з іншими протоколами IP-телефонії, протоколами ТМЗК, і для зв'язку з інтелектуальними мережами. [12]

Дизайн протоколу

Клієнти SIP традиційно використовують порт 5060 TCP і UDP для з'єднання елементів SIP-мережі. В основному, SIP використовується для встановлення і роз'єднання голосових і відеодзвінків. При цьому він може використовуватися і в будь-яких інших додатках, де потрібна установка з'єднання, таких, як системи оповіщення, мобільні термінали і так далі. Існує велика кількість рекомендацій RFC, що відносяться до SIP і визначають поведінку таких додатків. Для передачі самих голосових і відеоданих використовують інші транспортні протоколи, найчастіше Real-time Transport Protocol (RTP). [12]

Головним завданням розробки SIP було створення сигнального протоколу на базі IP, який міг би підтримувати розширений набір функцій обробки виклику і послуг, представлених в існуючій ТМЗК. Сам протокол SIP не визначає цих функцій, а зосереджений тільки на процедурах встановлення дзвінка і сигналізації. При цьому він був спроектований з підтримкою таких функціональних елементів мережі, як проксі-сервери (Proxy Servers) та Користувальницькі Агенти (User Agents). Ці елементи забезпечують базовий набір послуг: набір номера, виклик телефонного апарату, звукове інформування абонента про статус виклику. [12]

Телефонні мережі на основі SIP можуть підтримувати і більш сучасні послуги, що зазвичай надаються ЗКС №7, незважаючи на значну відмінність цих двох протоколів. ЗКС №7 характеризується складної, централізованої інтелектуальної мережею і простими, неінтелектуальними, терміналами (традиційні телефонні апарати). SIP - навпаки, вимагає дуже просту (і, відповідно, добре масштабується) мережу з інтелектом, вбудованим в кінцеві елементи на периферії (термінали, побудовані як фізичні пристрої або програми). [12]

SIP використовується разом з декількома іншими протоколами і бере участь тільки в сигнальної частини сесії зв'язку. SIP виконує роль носія для SDP, який описує параметри передачі відеоданих в рамках сесії, наприклад використовувані порти IP і кодеки. У типовому застосуванні сесії SIP - це просто потоки пакетів RTP. RTP є безпосереднім носієм голосових і відеоданих. [12]

Протокол SIP має клієнт-серверну архітектуру. Клієнт видає запити, із зазначенням того, що він хоче отримати від сервера. Сервер приймає і обробляє запити, видає відповіді, які містять повідомлення про успішність виконання запиту, повідомлення про помилку або інформацію, запитану клієнтом. [12]

Обслуговування виклику розподілено між різними елементами мережі SIP. Основним функціональним елементом, що реалізує функції управління з'єднанням, є абонентський термінал. Інші елементи мережі можуть відповідати за маршрутизацію викликів, а іноді служать для надання додаткових сервісів. [12]

Архітектура мережі на основі протоколі SIP показана на рисунку 2.2.

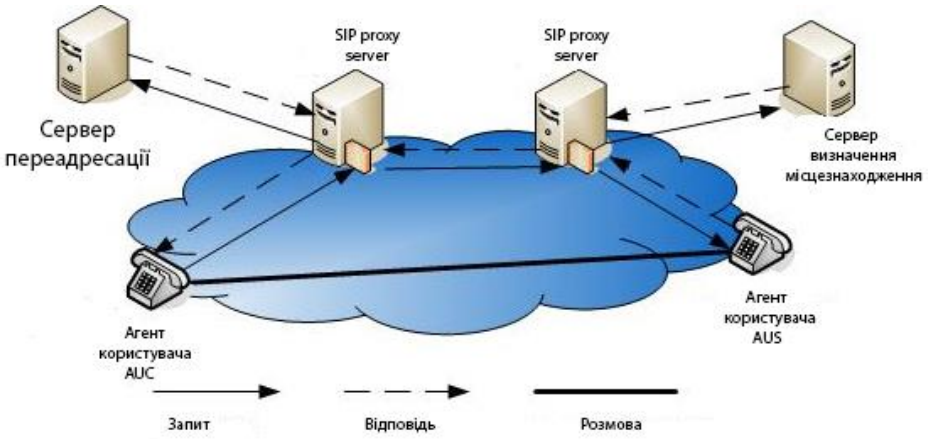


Рисунок - 2.2 Архітектура мережі на протоколі SIP

Термінал. У разі, коли клієнт і сервер взаємодіють безпосередньо з користувачем (тобто реалізовані в кінцевому обладнанні користувача), вони називаються, відповідно, клієнтом агента користувача - User Agent Client (UAC) - і сервером агента користувача - User Agent Server (UAS). [12]

Слід особливо відзначити, що сервер UAS і клієнт UAC можуть (але не зобов'язані) безпосередньо взаємодіяти з користувачем, а інші клієнти і сервери SIP цього робити не можуть. Якщо в пристрої присутні і сервер UAS, і клієнт UAC, то воно називається агентом користувача - User Agent (UA), а за своєю суттю є термінальне обладнання SIP. [12]

Проксі-сервер. Проксі-сервер (від англійського proxy - представник) представляє інтереси користувача в мережі. Він приймає запити, обробляє їх і, в залежності від типу запиту, виконує певні дії. Це може бути пошук і виклик користувача, маршрутизація запиту, надання послуг і т.д. Проксі-сервер складається з клієнтської і серверної частин, тому може приймати виклики, ініціювати власні запити і повертати відповіді. Проксі - сервер може бути фізично суміщений з сервером визначення місцеположення (в цьому випадку він називається REGISTRAR) або існувати окремо від цього сервера, але мати можливість взаємодіяти з ним по протоколам LDAP (RFC 1777), rwhois (RFC 2167) і по будь-яким іншим протоколам . [12]

Передбачено два типи проксі-серверів - зі збереженням станів (stateful) і без збереження станів (stateless).

Сервер першого типу зберігає в пам'яті вхідний запит, який став причиною генерації одного або декількох вихідних запитів. Ці вихідні запити сервер також запам'ятовує. Всі запити зберігаються в пам'яті сервера тільки до закінчення транзакції, тобто до отримання відповідей на запити.

Сервер першого типу дозволяє надати більшу кількість послуг, але працює повільніше, ніж сервер другого типу. Він може застосовуватися для обслуговування невеликої кількості клієнтів, наприклад, в локальній мережі. Проксі-сервер повинен зберігати інформацію про стани, якщо він:

- використовує протокол TCP для передачі сигнальної інформації;
- працює в режимі під LGPL сигнальної інформації;
- розмножує запити.

Останній випадок має місце, коли проксі-сервер веде пошук викликаного користувача відразу в декількох напрямках, тобто один запит, який прийшов до проксі-сервера, розмножується і передається одночасно по всіх цих напрямках.

Сервер без збереження станів просто ретранслює запити і відповіді, які отримує. Він працює швидше, ніж сервер першого типу, так як ресурс процесора не витрачається на запам'ятовування станів, внаслідок чого сервер цього типу може обслужити більшу кількість користувачів. Недоліком такого сервера є те, що на його базі можна реалізувати лише найбільш прості послуги. Втім, проксі-сервер може функціонувати як сервер зі збереженням станів для одних користувачів і як сервер без збереження станів - для інших. [12]

Алгоритм роботи користувачів з проксі-сервером виглядає наступним чином. Постачальник послуг IP-телефонії повідомляє адресу проксі-сервера своїм користувачам. Викликаючий користувач передає до проксі-сервера запит з'єднання. Сервер обробляє запит, визначає місце розташування викликаного користувача і передає запит цьому користувачеві, а потім отримує від нього відповідь, що підтверджує успішну обробку запиту, і транслює цю відповідь користувачеві, який надіслав запит. Проксі-сервер може модифікувати деякі заголовки повідомлень, які він транслює, причому кожен сервер, який обробив запит в процесі його передачі від джерела до приймача, повинен вказати це в

SIP-запиті для того, щоб відповідь на запит повернулася тим самим шляхом. [12]

Сервер переадресації. Сервер переадресації призначений для визначення поточної адреси викликаного користувача. Викликаючий користувач передає до сервера повідомлення з відомою йому адресою викликаного користувача, а сервер забезпечує переадресацію виклику на поточний адреса цього користувача. Для реалізації цієї функції сервер переадресації повинен взаємодіяти з сервером визначення місцеположення. [12]

Сервер переадресації НЕ термінує виклики як сервер RAS і не ініціює власні запити як проксі-сервер. Він тільки повідомляє адресу або викликає користувача, або проксі-сервер. За цією адресою ініціатор запиту передає новий запит. Сервер переадресації не містить клієнтську частину програмного забезпечення. [12]

Але користувачеві не обов'язково зв'язуватися з будь-яким SIP-сервером. Він може сам викликати іншого користувача за умови, що знає його поточну адресу. [12]

Сервер визначення місцеположення. Користувач може переміщатися в межах мережі, тому необхідний механізм визначення його місця розташування в поточний момент часу. Наприклад, співробітник підприємства виїжджає у відрядження, і всі виклики, адресовані йому, повинні бути спрямовані в інше місто на його тимчасове місце роботи. Про те, де він знаходиться, користувач інформує спеціальний сервер за допомогою повідомлення REGISTER. Можливі два режими реєстрації: користувач може повідомити свою нову адресу один раз, а може реєструватися періодично через певні проміжки часу. Перший спосіб підходить для випадку, коли термінал, доступний користувачеві, включений постійно, і його не переміщують по мережі, а другий - якщо термінал часто переміщається або вимикається. [12]

Для зберігання поточного адреси користувача служить сервер позиціонування користувачів, що представляє собою базу даних адресної

інформації. Крім постійної адреси користувача, в цій базі даних може зберігатися одна або кілька поточних адрес. [12]

Цей сервер може бути поєднаний з проксі-сервером (в такому випадку він називається registrar) або бути реалізований окремо від проксі-сервера, але мати можливість зв'язуватися з ним. [12]

В RFC 2543 сервер позиціонування представлений як окремий мережевий елемент, але принципи його роботи в цьому документі не регламентовані. Варто звернути увагу на те, що викликаючий користувач, якому потрібен поточна адреса викликаного користувача, безпосередньо не зв'язується з сервером визначення місцеположення. Цю функцію виконують SIP-сервери за допомогою протоколів LDAP (RFC 1777), rwhois (RFC 2167), або інших протоколів. [12]

2.3 Транспортні протоколі мережі SIP

У рамках мережі SIP можуть використовуватись різні транспортні протоколи. Розглянемо три основних протоколи.

2.3.1 Протокол UDP

Протокол User Datagram Protocol (UDP) використовує Інтернет-протокол для отримання блоку даних, який також називається датаграммой, з одного пристрою на інший через мережу. UDP - це полегшений протокол, так як не вимагає великого навантаження, пов'язаної з наявністю деталей на заголовку. Реклама послуг, таких як оновлення протоколів маршрутизації, доступність серверів і потокових додатків, таких як відео і голос, є одним з основних видів використання UDP. [21]

Для UDP використовується проста модель передачі даних. Це означає, що не існує гарантії цілісності та надійності даних, що забезпечує незахищеність, невпорядкованість, а іноді і дублювання датаграмм. На відміну від TCP, UDP

не сильно покладається на виправлення і перевірку помилок при виконанні. Таким чином, UDP добре підходить для мультікастінга або відправки всім абонентам, пакетного мовлення або відправки всім абонентам в локальній мережі. [22] UDP трафік, на відміну від TCP, не обов'язково вимагає відповіді і не обов'язково встановлювати з'єднання для відправки. [23]

UDP, на відміну від TCP, посилає пакети одержувачу незалежно від того, чи можуть він отримати їх повністю чи ні. Кожен з пакетів відправляється відправником одержувачу безпосередньо і індивідуально, без встановлення і підтвердження наявності надійного каналу передачі даних. Користувачам не надається можливість запитувати відсутні пакети даних після того, як вони втрачені при транспортуванні. [24] Даний тип протоколу використовується в основному в тих випадках, коли швидкість передачі даних має більш високий пріоритет, ніж надійність успішної передачі даних. Немає внутрішнього порядку передачі пакетів даних, і всі пакети передаються по мережі незалежно один від одного.

Як унікальний протокол, протокол User Datagram Protocol має свої плюси і мінуси. До переваг протоколу відноситься відносно вища швидкість передачі даних завдяки невеликій вазі пакетів з мінімальними заголовками. Так як протокол не потребує відповіді, він підходить для відеоконференцій, трансляцій та ігор. Але оскільки послідовність і підтвердження під час передачі даних відсутні, UDP вважається ненадійним та незахищеним. Пошкоджені пакети видаляються, а не запитуються для повторної передачі, після того як вони булизагублені.

Протоколи і порти

Кожному пристрою або комп'ютера в Інтернеті привласнений свій унікальний номер, відомий як IP-адреса. Інформація, передана через Інтернет з комп'ютера, тепер приймається за допомогою портів. Як і TCP, UDP також має свої специфічні функції і порти. Нижче наведені деякі з найбільш часто використовуваних для UDP.

Система доменних імен (DNS RFC 1034-1035: порт 53). Протокол DNS є одним із широко використовуваних протоколів як в публічних, так і в приватних мережах. Його основною метою є перетворення доменних імен в IP-адреси для маршрутизації по мережі. широко використовується в публічному інтернеті і приватних мережах для перетворення доменних імен в IP-адреси, зазвичай для маршрутизації мережі. DNS-сервери можуть бути налаштовані всередині приватної мережі, не будучи частиною глобальної системи.

Протокол динамічної конфігурації хоста (DHCP RFC 2 131: порт 67/68). Цей протокол в основному використовується в мережах, що не використовують статично призначені IP-адреси. Сервер може бути налаштований або інженером, або адміністратором, у якого є доступний для призначення пул адрес. Клієнт може включити пристрій і запросити IP-адреса з локального DHCP-сервера, і коли буде доступна адреса, вона буде призначена пристрою. Однак це не є постійним призначенням і закінчується через певний проміжок часу. Термін дії договору оренди закінчується, якщо не подається запит на продовження, і він буде повернутий в пул для передачі іншим пристроям.

Тривіальний протокол передачі файлів (TFP RFC 1 350: порт 69). Цей протокол, на відміну від звичайного протоколу передачі файлів, що використовується в TCP, пропонує метод передачі даних без створення сеансу. Використання протоколу TFTP не гарантує, що передача файлів була виконана належним чином. Цей протокол в основному використовується для оновлення мікропрограмного забезпечення та програмного забезпечення пристроїв.

Простий протокол мережевого управління (SNMP RFC 1901-1908, 3411-3418: порт 161- / 162). Цей протокол використовується для управління мережею. Можливість моніторингу, налаштування та управління мережевими пристроями - це деякі з можливостей SNMP.

Протокол мережевого часу (NTP RFC 5905: порт 123). Основною метою NTP є синхронізація пристроїв в Інтернеті, і вважається одним з найбільш ігнорованих протоколів. Для підтримки точних годин в більшості сучасних операційних систем використовується протокол NTP. Пристрій дозволяє без

особливих зусиль усувати неполадки на різних пристроях, оскільки годинник точний, що робить NTP життєво важливою частиною мережевих систем. [27]

На закінчення слід додати, що на сьогоднішній день UDP виконує свою власну задачу разом з різними інтернет-протоколами. Він все ще використовується в багатьох основних додатках, які ми використовуються щодня, наприклад, для потокової передачі відео і відеоконференцій, що стало особливо затребуваним в умовах пандемії коронавірусу.

2.3.2 Протокол TCP

Протокол TCP (transmission control protocol) - це набір протоколів, який задає стандарти зв'язку між комп'ютерами і містить докладні угоди про маршрутизації і міжмережевої взаємодії. TCP забезпечує зв'язок підключених до мережі комп'ютерів, зазвичай званих хостами. Будь-яку мережу можна підключити до іншої мережі і організувати зв'язок з її хостами. Незважаючи на те, що існують різні мережеві технології, багато з яких засновані на комутації пакетів і потоковому режимі передачі, набір протокол TCP має однією істотною перевагою: він забезпечує апаратну незалежність. [28]

Так як в протоколах Internet визначається тільки блок передачі і спосіб його відправки, TCP не залежить від особливостей мережевого апаратного забезпечення, дозволяючи організувати обмін інформацією між мережами з різною технологією передачі даних. Система IP-адрес дозволяє встановити з'єднання між будь-якими двома машинами мережі. Крім того, в TCP / IP також визначені стандарти для багатьох служб зв'язку, призначених для кінцевих користувачів. [28]

TCP на відміну від UDP здійснює доставку дейтограмм, званих сегментами, у вигляді байтових потоків з встановленням з'єднання. Протокол TCP застосовується в тих випадках, коли потрібно гарантована доставка повідомлень. Він використовує контрольні суми пакетів для перевірки їх цілісності та звільняє прикладні процеси від необхідності таймаутів і повторних

передач для забезпечення надійності. Найбільш типовими прикладними процесами, що використовують TCP, є FTP (File Transfer Protocol - протокол передачі файлів) і telnet. Крім того, TCP використовують системи SMTP, HTTP, X-window, RCP (remote copy), а також "r"-команда. Внутрішня структура модуля TCP набагато складніше структури UDP. Подібно до того, як UDP прикладні процеси взаємодіють з модулем TCP через порти. Під байтовими потоками тут мається на увазі те, що один примітив, наприклад read, може викликати посилку адресату послідовності сегментів, які утворюють певний блок даних (повідомлення). Використання портів відкриває можливість здійснювати кілька з'єднань між двома мережевими об'єктами (працювати з різними процесами). [28]

2.3.3 Протокол SCTP

SCTP (Stream Control Transmission Protocol - протокол передачі з керуванням потоку) - протокол транспортного рівня. Виконує ті ж функції, що і протоколи TCP і UDP. Але об'єднує при цьому їх переваги, позбавляє недоліків і додає нові можливості. [29]

Основні відмінності між протоколами UDP, TCP та SCTP наведено у таблиці 2.1:

Таблиця 2.1 - Порівняння характеристик протоколів UDP, TCP та SCTP

	UDP	TCP	SCTP
Встановлення з'єднання	Ні	Так	Так
Надійна передача	Ні	Так	Так
Збереження меж повідомлень	Так	Ні	Так

Продовження таблиці 2.1

Впорядкована доставка	Ні	Так	Так
Неупорядкована доставка	Так	Ні	Так
Розмір контрольної суми даних (біт)	16	16	32
Шлях MTU	Ні	Так	Так
Управління накопиченням	Ні	Так	Так
Багатопотоковість	Ні	Ні	Так
Підтримка більшості інтерфейсів	Ні	Ні	Так
Зв'язка потоків	Ні	Так	Так

Основні переваги протоколу SCTP (пояснення до таблиці):

Збереження меж - в протоколі TCP дані передаються безперервним потоком байт, читаються так само, тому адміністратор повинен сам стежити за тим, як розставляти кордони в цьому потоці і обробити шматки даних. SCTP дозволяє ставити кордони і обробляти дані пакетами, як в UDP. Але при цьому гарантує порядок доставки пакетів, забезпечує надійність і орієнтований на з'єднання. Впорядкованість пакетів, до речі, можна відключити для підвищення швидкості. [29]

Multihoming (Багатолінійні, множинна адресація) - SCTP дозволяє встановлювати з'єднання до одного сервера по різних лініях зв'язку (наприклад, по Wi-Fi і по Ethernet). Таким чином, якщо одна лінія зв'язку стане недоступною (наприклад, мережа Wi-Fi), то з'єднання не розірветься. Це так

само дозволяє передавати дані відразу по декількох лініях, що збільшує швидкість передачі. Якщо в TCP одна лінія зв'язку обірветься, то з'єднання буде втрачено, доведеться встановлювати нове. [29]

На рисунку 2.3 показано схему доставки повідомлень протоколами TCP та SCTP.

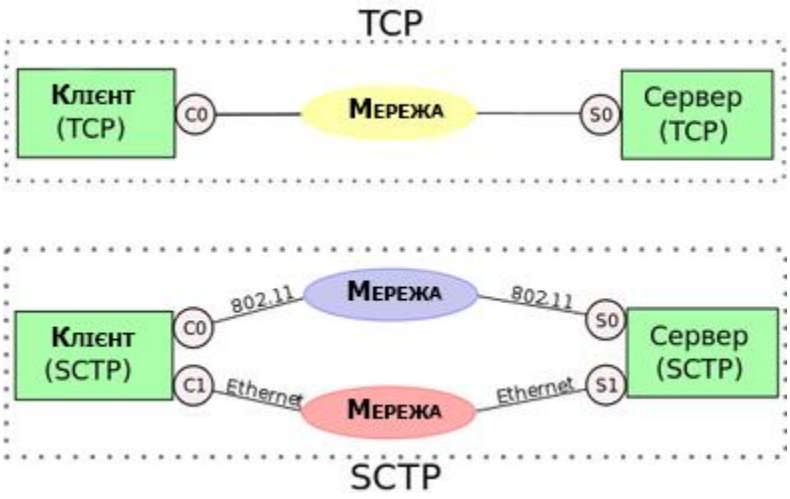


Рисунок 2.3 - Схема доставки повідомлень протоколами TCP та SCTP

Multithreading (багатопоточність) - дозволяє передавати кілька потоків в рамках однієї сесії (сесією в SCTP називається з'єднання між двома хостами). Наприклад в TCP дані та службова інформація передаються по одному з'єднанню. Тому затримка в отриманні службовою інформацією може бути викликана поточною передачею даних (наприклад, ACK може не прийти вчасно, тому будуть відправлені дублікати). Така проблема називається head-of-line blocking, HOL. Багатопоточність дозволяє передавати ці дані незалежно, що приведе до кращого використання доступних ресурсів. [29]

4-way handshake - протокол TCP схильний SYN-flood атакам. Зловмисник шле багато пакетів в короткий час для запиту TCP з'єднання (запит на з'єднання позначений бітом SYN в заголовку, тому і SYN-flood). Але при цьому не підтверджує встановлення з'єднання. Таким чином на сервері утворюються напіввідкриті з'єднання. Вони закриваються самі по закінченню таймаута. Але мета зловмисника полягає в тому, щоб створити якомога більше таких сполук,

не даючи тим самим створювати нові з'єднання через обмеження в їх кількості на стороні сервера (сервер не може мати нескінченну кількість з'єднань, а якщо зробити таймаут на обрив занадто маленьким , то підтвердження з'єднання можуть відхилятися завчасно, що теж недобре, і це все робить SYN-атаки можливими). У SCTP використовується не потрійне рукостискання, а четверне (з розряду: "я хочу встановити з'єднання - ти точно хочеш з'єднатися? - так, я точно хочу встановити з'єднання – добре, встановлюємо з'єднання"). Таким чином за короткий проміжок часу можна створити багато нових з'єднань. [29] Схема встановлення з'єднання протоколами TCP та SCTP показано на рисунку 2.4.

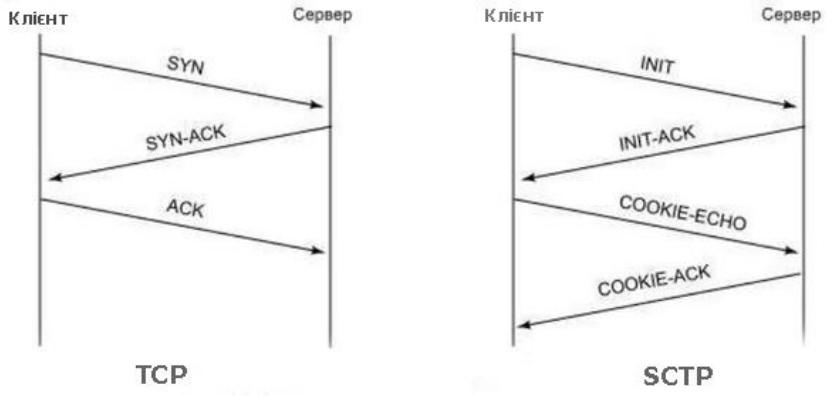


Рисунок 2.4 - Схема встановлення з'єднання протоколами TCP та SCTP

У SCTP не буває напівзакритих з'єднань, як в TCP. Якщо ми закриваємо з'єднання, то відразу в обидві сторони.

На жаль, незважаючи на всі переваги, протокол SCTP не отримав поки широкого поширення. Це пов'язано з інертністю (поки старі протоколи TCP та UDP працюють, немає потреби їх замінювати), та складністю підтримки на апаратному рівні (наприклад, вся обгортка мережевих протоколів, ті ж фаєрволи, мають правила пропускання тільки UDP та TCP пакетів).

2.4 Висновки до розділу 2

Підсумовуючи, слід зазначити, що протокол SCTP гарантує доставку пакетів, та зі збереженням їх правильної послідовності, на відміну від протоколу UDP, який зовсім не гарантує доставку повідомлень, та на відміну від протоколу TCP, який передає потік байтів, та може страждати від ефекту блокування головного рядка. Саме ця характеристика робить протокол найвигіднішим протоколом для організації взаємодії мережі SIP та мережі з інтеграцією послуг. Можливість використання протоколу SCTP як транспортного протоколу для вирішення данної задачі досліджено в наступних розділах.

3 АЛГОРИТМ ВЗАЄМОДІЇ МЕРЕЖІ SIP ТА МЕРЕЖІ З ІНТЕГРАЦІЄЮ ПОСЛУГ ПІД ЧАС НАДАННЯ СЕАНСУ ГОЛОСОВОГО ЗВ'ЯЗКУ

Існує два основних шляхи взаємодії мереж ЗКС №7 та NGN на базі IMS в залежності від мережі відправника та мережі кінцевого отримувача трафіку. Ці два алгоритми зв'язку мають назву інкапсуляція та трансляція трафіку, і ці механізми розглянуті у моїй роботі.

3.1 Інкапсуляція повідомлень ISUP в SIP

Інкапсуляція сигналізації ТМЗК є одним з основних вимог до SIP-T. Протокол SIP-T використовує розділення на необхідне число частини MIME для того, щоб повідомлення SIP могли містити в собі різноманітну корисну інформацію (дані протоколів SDP, ISUP, і т.д.). В даний час існують численні версії ISUP і тому для того, щоб визначити, який використовується варіант, введений спеціальний тип MIME - ISUP Media Type, і це дозволяє зручно отримати інформацію про використаний варіанті протоколу ISUP. [3]

Прозорий транзит для повідомлень ISUP. Щоб дозволити шлюзам отримати перевагу повного набору послуг, що надається існуючою телефонною мережею при встановленні викликів від ТМЗК до ТМЗК через мережу SIP, повідомлення SIP повинні бути здатні до транспортування корисного навантаження ISUP від шлюзу до шлюзу. Агентам користувача SIP, які не розуміють ISUP, дозволяється ігнорувати опціональні тіла MIME. [3]

Розуміння багатоскладових тіл MIME. У більшості ситуацій взаємодії ТМЗК, тіла повідомлень SIP будуть нести інформацію опису сеансу (SDP), як додаткову до ISUP та/або білінгової інформації. Вузли взаємодії ТМЗК повинні розуміти тип MIME багаточастинний /змішаний (multipart/mixed), як визначено в RFC2046. Клієнти висловлюють підтримку цього, шляхом включення multipart/mixed в заголовок Accept. [3]

Узгодження змісту SIP. Ініціатор запиту SIP-T повинен упакувати обидва елементи SDP і ISUP в одне й те саме повідомлення SIP, використовуючи формат MIME. У SIP прийнято, що якщо термінальний пристрій не підтримує багаточастинне навантаження (багаточастинне/змішане) або конкретний тип ISUP MIME, то він повинен відхилити цей запит SIP відповіддю 415 (Unsupported Media Type - тип медіа-з'єднання не підтримується) із зазначенням підтримуваних типів методів з'єднання (за замовчуванням, application/SDP). Потім ініціатор повинен знову послати запит SIP, прибравши з нього навантаження ISUP (тобто тільки з навантаженням SDP), і тоді він буде прийнятий. [3]

Це досить громіздка процедура, і тому вкрай бажано мати механізм, за допомогою якого ініціатор міг би помітити обов'язкові і необов'язкові елементи так, щоб приймаюча сторона могла просто відкидати необов'язкові елементи, які вона не розуміє (дозволяючи телефону SIP ігнорувати навантаження ISUP, якщо її обробка не є критичною). Це можливо, якщо приймаюча сторона має підтримку багаточастинного/змішаного типу вмісту (Content-type) і доступ до заголовку розташування вмісту (Content-Disposition) для виявлення критичності.

Підсумовуючи, обидва варіанти взаємодії SIP та ISUP, та вимагають підтримку цілого ряду параметрів, значень та можливостей. Також, враховуючи той факт, що, як раніше було сказано, що для взаємодії вище згаданих протоколів потрібна підтримка одразу обох способів, це ще більше ускладнює задачу взаємодії. Протокол SIP-T в даній взаємодії відіграє основну роль, та може вирішити одразу дві задачі – інкапсуляцію та трансляцію. [3]

3.2 Трансляція повідомлень ISUP в SIP

Трансляція включає в себе всі аспекти перетворення протоколу сигналізації між SIP і ISUP. До проблеми трансляції відносяться по суті два компоненти:

Відображення повідомлення ISUP на SIP. Воно описує відповідність між ISUP і SIP на рівні повідомлень. При реалізації SIP-T на шлюзи покладається завдання створення спеціального повідомлення ISUP для кожного одержуваного повідомлення SIP і виконання зворотної функції. Це необхідно для визначення правил, що регулюють відповідність між повідомленнями ISUP і SIP (тобто, які повідомлення ISUP надсилаються, коли отримано конкретне повідомлення SIP: IAM має бути надіслано при отриманні INVITE, REL при отриманні BYE і так далі). [3]

Відображення параметрів ISUP на заголовок SIP. Запит SIP, який використовується для встановлення телефонного з'єднання, повинен містити інформацію, що забезпечуватиме йому правильну маршрутизацію до місця призначення проксі-серверами мережі SIP - наприклад, номер телефону, набраний викликаючим користувачем. Це важливо для стандартизації набору правил, що визначають процедуру трансляції інформації ISUP в SIP (наприклад, номер викликаної сторони (Called Party Number) в ISUP IAM повинен бути відображений в полі заголовку «To» і в Request-URI протоколу SIP, і т.п.). Це завдання стає значно складнішим, якщо врахувати, що заголовки запиту SIP (і зокрема INVITE) можуть бути зміненими в проміжних пунктах, в результаті чого заголовки SIP і інкапсульовані частини ISUP можуть видавати суперечливі один одному значення - фактично частина інкапсульованого ISUP може вважатися непотрібною і застарілою. В такому випадку пріоритет буде надаватися значенню заголовків, тобто при створенні нового повідомлення параметри заповнюються значеннями із заголовків запиту SIP, а відсутня інформація буде запозичена з вкладеного повідомлення ISUP, якщо воно присутнє. [3]

3.3 Процес встановлення з’єднання між ISUP та SIP

В цьому розділі буде розглянуто декілька основних сценаріїв встановлення з’єднання між ISUP та SIP. На наведених нижче діаграмах

показано порядок повідомлень в типових успішних і позаштатних ситуаціях встановлення виклику з боку мережі ТМЗК. [3]

На цих схемах всі тони дзвінка (SIP, ISUP) проходять через MGCF, а обробку медіа-інформації здійснює MG під керуванням MGCF. Для простоти вони показані у вигляді єдиного пристрою, позначеного як MGCF/MG. [3]

Процес встановлення виклику при сигналізації блоком (відповідь неавтоматична) показано на рисунку 3.1.

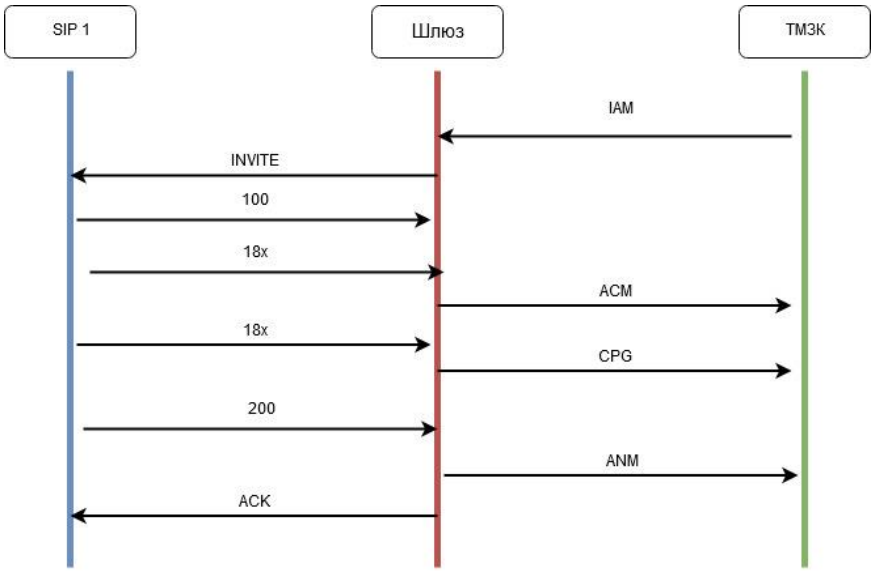


Рисунок 3.1 - Встановлення виклику (відповідь неавтоматична)

1. Коли абоненту ТМЗК потрібно почати встановлення сеансу з абонентом SIP, ТМЗК генерує повідомлення IAM в напрямку шлюзу.

2. При прийомі повідомлення IAM шлюз генерує повідомлення INVITE і надсилає його відповідного вузла SIP.

3. Якщо відбувається така подія, що показує достачу адресної інформації виклику, то вузлом SIP генерується відповідь 180 (або більша).

4. При прийманні попередньої відповіді 180 або більшої шлюз генерує повідомлення ACM. Якщо відповідь була не 180, то в повідомленні ACM значення called party status (статус викликаної сторони) буде показаний no indication (не вказано).

5. Вузол SIP може і далі використовувати попередні повідомлення для індикації ходу сеансу.

6. Після того, як повідомлення ACM послано, всі попередні відповіді транслюються в повідомлення ISUP CPG.

7. Коли вузол SIP відповість на виклик, він надсилає повідомлення 200 OK.

8. При прийомі повідомлення 200 OK шлюз надсилає повідомлення ANM в напрямку вузла ISUP.

9.Для підтвердження прийому завершуючої відповіді на INVITE шлюзом надсилається повідомлення ACK вузлу SIP. [3]

Процес встановлення виклику з автоматичною відповіддю показано на рисунку 3.2.

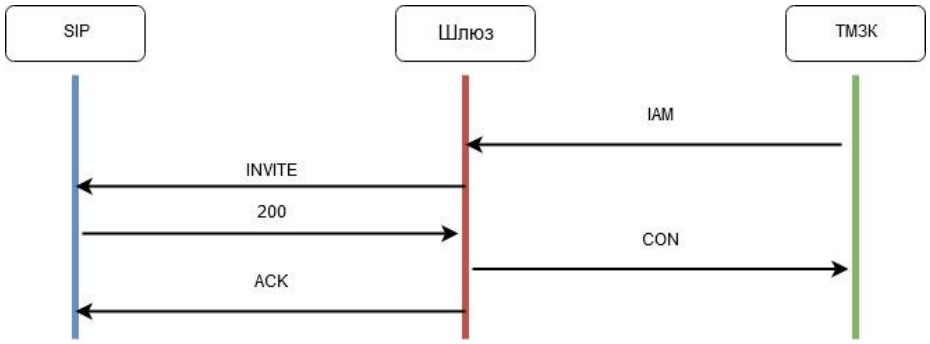


Рисунок 3.2 - Встановлення виклику (відповідь автоматична)

1. Коли абоненту ТМЗК потрібно почати встановлення сеансу з абонентом SIP, ТМЗК генерує повідомлення IAM в напрямку шлюзу.

2. При прийомі повідомлення IAM шлюз генерує повідомлення INVITE і надсилає його до відповідного вузла SIP на основі аналізу номера абонента, що викликається.

3. Так як вузол SIP встановлений в режим автоматичної відповіді на виклик, то він надсилає повідомлення 200 OK.

4. Після отримання повідомлення 200 OK шлюз надсилає повідомлення CON в напрямку вузла ISUP.

5. Для підтвердження прийому остаточної відповіді на INVITE шлюз надсилає повідомлення ACK вузлу SIP. [3]

Процес закінчення часу відповіді SIP показано на рисунку 3.3.

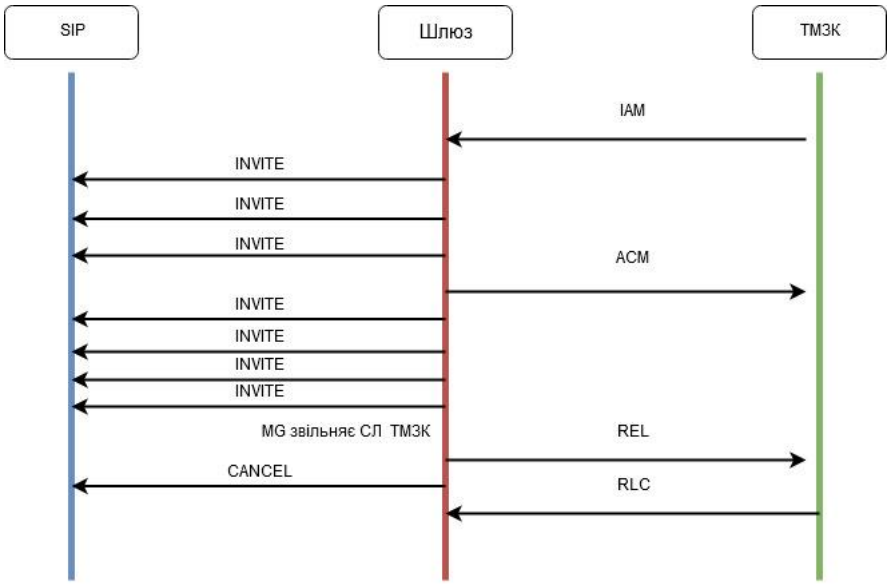


Рисунок 3.3 - Закінчення часу відповіді SIP

1. Коли абоненту ТМЗК потрібно почати встановлення сеансу з абонентом SIP, ТМЗК генерує повідомлення IAM в напрямку шлюзу.

2. При прийомі повідомлення IAM шлюз генерує повідомлення INVITE і надсилає його до відповідного вузла SIP на основі аналізу номера абонента, що викликається. У цей час проводиться установка таймера T11 для ISUP і таймера T1 для SIP.

3. Кожен раз після закінчення часу таймера T1 вузлу SIP надсилається повідомлення INVITE. За стандартом SIP передбачається проводити передачу повідомлення INVITE 7 разів, якщо немає прийому відповіді.

4. Після закінчення часу таймера T11 вузлу ISUP буде надіслано повідомлення ACM для запобігання скидання ACM значення called party status (статус викликаної сторони) буде вказано no indication (не вказано).

5. Після того, як максимальне число запитів INVITE буде передано, шлюз відправить REL (код причини 18) вузлу ISUP для завершення виклику.

6. Окрім того, шлюз передає повідомлення CANCEL вузлу SIP для завершення будь-яких спроб ініціації.

7. При прийомі REL віддалений вузол ISUP в якості підтвердження передає повідомлення RLC. [3]

Процес прийому відповіді SIP з індикацією помилки показано на рисунку 3.4.

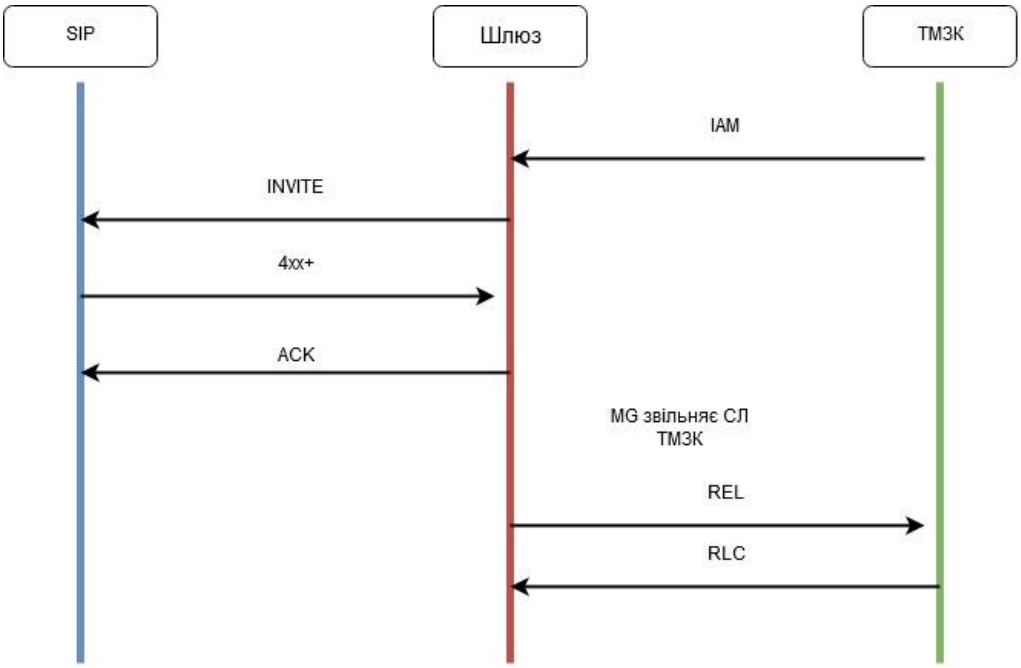


Рисунок 3.4 - Відповідь SIP з індикацією помилки

1. Коли абоненту ТМЗК потрібно почати встановлення сеансу з абонентом SIP, ТМЗК генерує повідомлення IAM в напрямку шлюзу.

2. При прийомі повідомлення IAM шлюз генерує повідомлення INVITE і надсилає його до відповідного вузла SIP на основі аналізу номера викликаного абонента.

3. Вузол SIP вказує на стан помилки у відповідь повідомленням з кодом 400 або більшим.

4. Для підтвердження прийому остаточної відповіді на INVITE шлюз надсилає повідомлення ACK вузлу SIP.

5. Повідомлення REL ISUP генерується з вузла SIP.

6. Віддалений вузол ISUP, після підтвердження прийому повідомлення REL, надсилає повідомленням RLC. [3]

Процес перенаправлення в SIP показано на рисунку 3.5.

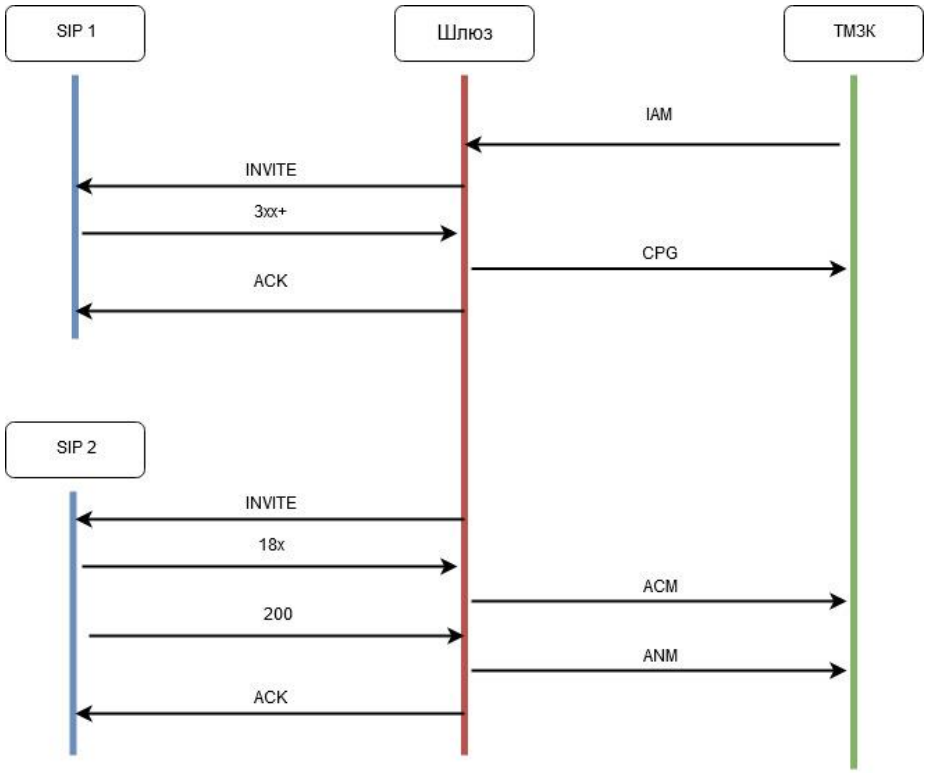


Рисунок 3.5 - Перенаправлення в SIP

1. Коли абоненту ТМЗК потрібно почати встановлення сеансу з абонентом SIP, ТМЗК генерує повідомлення IAM в напрямку шлюзу.

2. При прийомі повідомлення IAM шлюз генерує повідомлення INVITE і надсилає його до відповідного вузла SIP на основі аналізу номера абонента, що викликається.

3. Вузол SIP посилкою повідомлення 3xx вказує, що ресурс, з яким користувач намагається встановити контакт, розташований в іншому місці. У таких випадках ми припускаємо, що контактний URL дійсний і є доступним для VoIP SIP викликом.

4. Шлюз передає CPG з індикацією події перенаправлення виклику при прийомі повідомлення 3xx. Зауважимо, що повинна бути можливість

скасування такої трансляції через конфігурацію, так як деякі вузли ISUP не підтримують прийом повідомлень CPG до повідомлень ACM.

5. Для підтвердження прийому остаточної відповіді на INVITE, шлюз відправляє повідомлення ACK вузлу SIP.

6. Шлюз відправляє прийняте повідомлення INVITE за адресою, зазначеною в поле контакту повідомлення 3xx.

7. Коли відбувається подія, яка свідчить що у виклика є достатня адресна інформація, вузол SIP генерує попередню відповідь 180 або більшу.

8. При прийманні попередньої відповіді 180 або більшої шлюз генерує повідомлення ACM з кодом події.

9. Коли вузол SIP відповідає на виклик, він надсилає повідомлення 200 OK.

10. Після отримання повідомлення 200 OK шлюз надсилає повідомлення ANM в напрямку вузла ISUP.

11. Для підтвердження прийому остаточної відповіді на INVITE шлюз надсилає повідомлення ACK вузлу SIP. [3]

Процес скасування виклику з боку ISUP показано на рисунку 3.6.

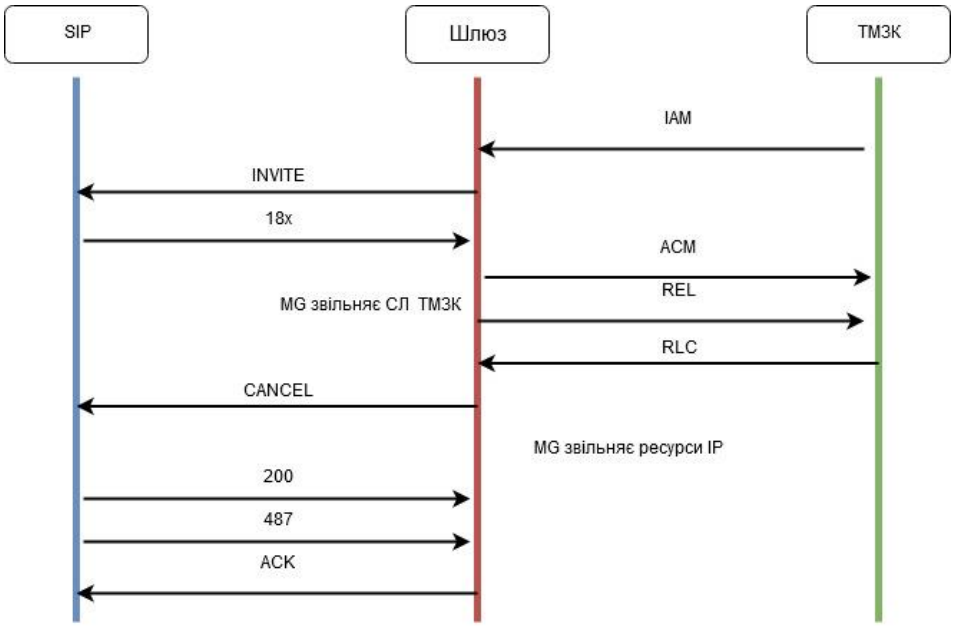


Рисунок 3.6 - Скасування виклику з боку ISUP

1. Коли абоненту ТМЗК потрібно почати встановлення сеансу з абонентом SIP ТМЗК генерує повідомлення IAM в напрямку шлюзу.

2. При прийомі повідомлення IAM шлюз генерує повідомлення INVITE і надсилає його до відповідного вузла SIP на основі аналізу номера викликаного абонента.

3. Коли відбувається подія, свідчить що у виклика є достатня адресна інформація, вузол SIP генерує попередню відповідь 180 або більшу.

4. При прийманні попередньої відповіді 180 або більшої шлюз генерує повідомлення ACM, в яке записує код події.

5. Якщо абонент розірве з`єднання раніше, ніж надійде відповідь від вузла SIP, то буде згенероване повідомлення REL.

6. Шлюз звільняє лінію ТМЗК надсилаючи повідомлення RLC, тим самим показує, що лінія доступна для нового використання.

7. При прийомі повідомлення REL до заключної відповіді на INVITE шлюз посилає CANCEL в напрямку вузла SIP.

8. При прийомі CANCEL вузол SIP посилає відповідь 200.

9. Віддалений вузол SIP посилає 487 Call Cancelled для завершення передачі INVITE.

10. Для підтвердження прийому завершуючої відповіді на INVITE шлюзом надсилається повідомлення ACK вузлу SIP. [3]

Всі ці задачі є прикладом варіантів створення з’єднання, і, як видно з приведених прикладів, в залежності від ситуації, потрібно розпізнавати отриманні повідомлення однієї мережі, аналізувати їх, зіставляти їх з повідомленнями іншої мережі, і, знайшовши відповідний варіант, продовжувати сигналізацію, при цьому роблячи цей процес безперервним і точним. Будь яка неправильна інтерпретація повідомлень може порушити весь процес сигналізації, що приведе до невиконання запиту користувача. Цей об’єм роботи, а також кількість покладених задач, робить роль протоколу SIP визначною в взаємодії мереж ЗКС7 та NGN на базі IMS.

3.4 Висновки до розділу 3

В даному розділі були розглянуті механізми взаємодії телефонної мережі загального користування та мережі SIP. Забезпечення гарантованої та послідовної доставки повідомлень, при передачі трафіку підсистеми ISUP мережею SIP, є одним із найважливіших аспектів даної взаємодії. Протокол SCTP являється саме тим механізмом, що може забезпечити як гарантованість доставки повідомлень, так і збереження їх послідовності, на відміну від розповсюджених протоколів UDP та TCP, і в цьому аспекті застосування протоколу SCTP дало б приріст в якості обслуговування абонентів. Але чи будуть інші показники продуктивності мережі (наприклад, пропускна здатність та затримка при втраті частини пакетів) кращими при використанні протоколу SCTP в умовах трансляції трафіку підсистеми ISUP мережею SIP, досліджено в наступному розділі.

4 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ВЗАЄМОДІЇ МЕРЕЖІ SIP ТА МЕРЕЖІ ISDN ПРИ ВИКОРИСТАННІ ПРОТОКОЛІВ UDP ТА SCTP

SIP (Session Initiation Protocol), розроблений IETF для VoIP-сигналізації, є протоколом управління зв'язком, здатний працювати на різних транспортних рівнях, наприклад, TCP, UDP або SCTP. Сучасна програма SIP працює здебільшого через ненадійному транспортному протоколі UDP. У середовищі з втратами, такому як бездротові мережі зв’язку, SIP-повідомлення можуть бути втрачені або доставлені не в порядку. Потім програма SIP повинна повторно передати втрачені повідомлення та змінити порядок отриманих пакетів. Такі додаткові накладні витрати на обробку можуть погіршити продуктивність роботи протоколу SIP. А в умовах, коли протокол SIP є зв’язковим елементом між технологіями NGN та ЗКС№7, коли друга технологія є технологією з комутацією каналів, задача повторної передачі втрачених пакетів інформації ще більш ускладнює, і без того не легку, задачу взаємодії цих двох технологій. Тому для вирішення цієї проблеми дослідники шукають більш Відповідний протокол транспортного рівня для SIP.

SCTP, транспортний протокол, що забезпечує підтверджену, безпомилкову, не дубльовану передачу повідомлень, пропонується стати альтернативою UDP і TCP. Функції багатопотокової передачі та багатокористувацького самонаведення SCTP особливо привабливими для випадків, які мають жорсткі вимоги до продуктивності та високої надійності з’єднання.

4.1 Загальна інформація про моделювання

Всі моделювання проводяться за допомогою мережевого симулятора NS-3.

Симулятор ns-3 - програмний продукт для моделювання мереж, що розроблявся в Каліфорнійському університеті з 1989 року. Ця програма

безкоштовно розповсюджується в відкритих кодах на умовах ліцензії GPL (GNU Public License), і доступна для більшості сучасних операційних систем. Даний симулятор здійснює імітаційне моделювання мереж на рівні пакетів, а саме моделює генерацію пакетів та проходження їх по мережі. На прикладному рівні моделюється характер трафіку, який проходить різними додатками: Web, FTP, Telnet, RealAudio. Також можливе моделювання роботи протоколів транспортного рівня UDP та різних реалізацій TCP, багатоадресних протоколів, різних протоколів маршрутизації в провідних та безпровідних мереж. Крім того, моделюються деякі фактори, що відносяться до фізичного рівня: затримка пакетів у каналах, виникнення помилок, видимість/невидимість вузлів у безпровідних мережах, та багато інших параметрів.

Результатом роботи симулятора є вихідні текстові файли, в яких реєструється хід моделювання (моменти генерації/отримання пакети, стан черг, і т. д.). Крім того, в модель може бути включена в інструкції, які ідентифікують будь-які величини, вимірювання яких вимагається в конкретному завданні (затримка пакетів, пропускна здатність і т. п.). Значення цих величин у ході моделювання також можна зареєструватися у вихідних файлах. Для візуалізації результатів служать аніматор NAM (Network Animator) і будівник графіків Xgraph. Крім того, система містить генератор топологій, що спрощує опис топології великих мереж.

Перейдемо до моделювання. На рисунку 4.1 показана топологія мережі, яка була використована при моделюванні. Вузли 1 і 2 є маршрутизаторами, в яких обмежений буфер. Вузли 4 і 5 являються джерелом TCP і потік, відповідно, що несуть трафік FTP, який був використаний в даному сценарії. Вузли 0 і 3 імітують об'єкти SIP (а саме MCG), що обмінюються повідомленнями SIP при активному сеансі. Єдиним вузьким місцем для трафіку було між вузлами 1 і 2 , яке було спільне для обох кінцевих точок відправників 0 і 4, які конкурували у даному експерименті. Так як реальний сценарій може давати більшу кількість проміжних стрибків, то пропускна здатність в даному вузькому місці вибирається для забезпечення великих спостережень. Значення

затримок вибрані таким чином, щоб загальна затримка була рівна 45 мс, що являє собою затримку передачі між SIP-серверома у Європі та у США.

Модельований випадок обміну повідомленнями SIP включає проблеми з перевантаженнями трафіку та конкуренцією трафіку на шляху руху, оскільки передаються сигнали ТМЗК через IP без участі будь-якої кінцевої точки, яка знаходиться на IP. Генерування трафіку досягається за допомогою стаціонарної моделі Poission (зазвичай використовується для телефонії), що генерує SIP-повідомлення розміром 578 байт у вузлі 0. Запроси INVITE, які надходять до вузла 0, переадресовуються до вузла 1, який спочатку відповідає повідомленням 100, а пізніше 180. Відповідь повертається, коли буде отримано дзвінок з мережі ТМЗК. Швидкість формування запитів рівна 10 Мб/с, що буде половиною від загальної швидкості. Це обумовлено тим, що у випадку SIP-T MGC не тільки може надіслати запити INVITE, але й ACK/200OK, тому швидкість створення трафіку додатків подвоюється, і буде становити 20 Мб/с

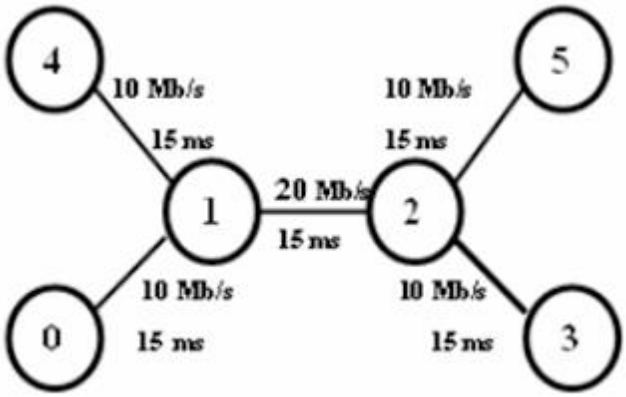


Рисунок 4.1 - Топологія мережі

Основним спостереженням є затримка INVITE та відповідна реакція дзвінка з використанням UDP та SCTP за різних умов. Також пропускна здатність обчислюється в доповнення до затримок з постійною конкуренцією трафіку за вузьким місцем зв'язку та різними розмірами буфера на маршрутизаторі.

4.2 Проведення дослідження

Для аналізу затримок, запропонованих транспортними протоколами, моделюються два базових сценарії. Один - вивчити вплив перехресного трафіку на затримки, а другий - спостерігати вплив різних умов втрати пакетів на затримки.

4.2.1 Конкуруючий трафік

Цей тест призначений для оцінки впливу на затримки, спричинені перехресним трафіком між вузлом 4 і 5, щоб змусити вузол 0 і вузол 4 конкурувати за пропускну здатність на вузькому місці. Повідомлення SIP генеруються проксі-сервером у вузлі 0, і негайно пересилаються на вузол 3. Перехресний трафік у вузлі 4 генерується за допомогою TCP. Час, коли SIP-повідомлення INVITE розміщується в черзі на транспортному рівні у вузлі 0, віднімається з часу, коли воно доставляється до програми у вузлі 3, щоб отримати затримку для конкретного запиту INVITE. Результати моделювання показано на рисунку 4.2.

Трафік у вузлі 4 за допомогою TCP генерується лише протягом певного періоду часу. Результати цього тесту показані на малюнку 4.2. Вісь X показує номер послідовності повідомлень, тоді як вісь у показує час, який потрібно повідомленням INVITE SIP для досягнення пункту призначення. Видно, що не спостерігається істотно великої різниці у затримках, досягнутих обома транспортними протоколами. SCTP дійсно стикається з ситуацією, при якій пакети мають затримку до 800 мс при невеликій кількісті послідовності, але на досить короткий час. У випадку UDP затримки залишаються незмінними, оскільки це основний атрибут UDP. Він показує великі смуги лише при повторній передачі пакетів. Можливо, це найбільший недолік використання UDP поряд з багатьма перевагами, які особливо сприятливі для випадку телефонної сигналізації. Загальний результат цього експерименту полягає в

тому, що як UDP, так і SCTP працюють добре, хоча затримки, які спостерігає SCTP, є трохи вищі, але все одно не суттєво насторожують.

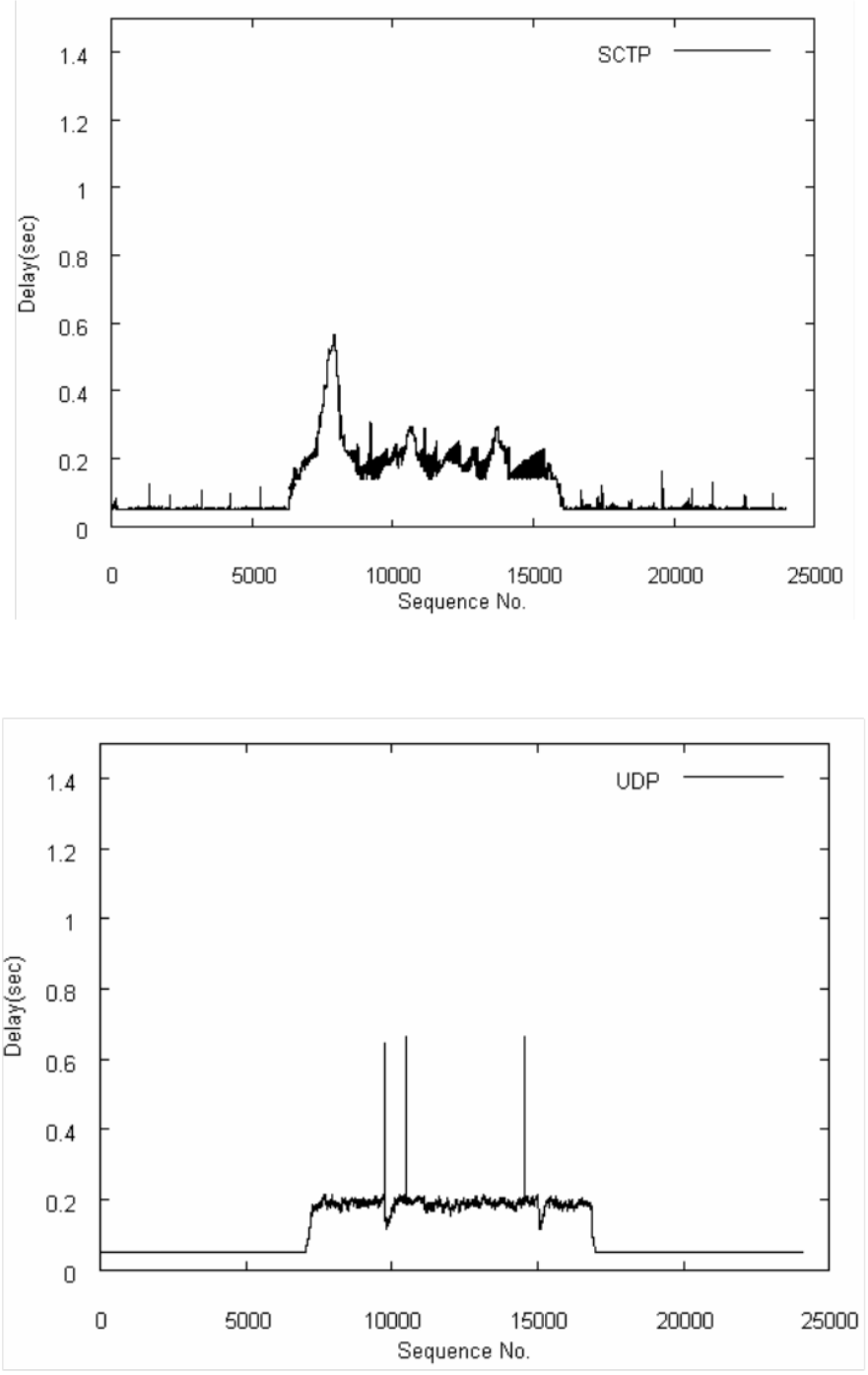


Рисунок 4.2 - Вплив конкуруючого трафіку

4.2.2 Ефект втрати пакетів

Для порівняння продуктивності UDP і SCTP в умовах втрати пакетів зроблено три моделювання як для UDP, так і для SCTP. У вузлі 1 моделювалися випадкові коефіцієнти втрати пакетів у розмірі 0,1, 0,2 та 0,3%. На рисунку 4.3 показано продуктивність протоколів при втраті 0..1% пакетів

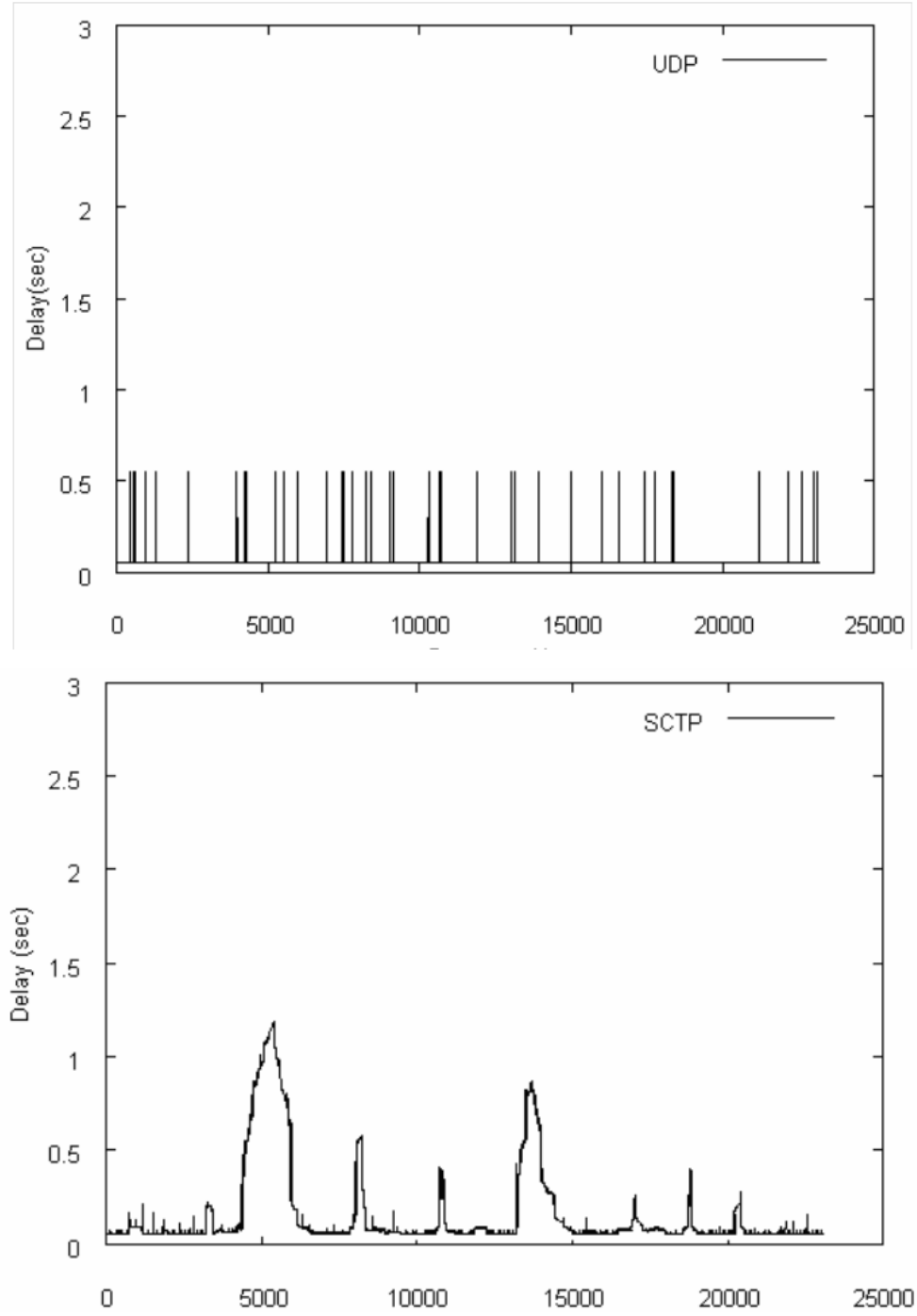


Рисунок 4.3 - Продуктивність протоколів при втраті 0.1% пакетів

Показники, що використовуються для розрахунків затримки, такі ж, як описані в попередньому експерименті. Результати цікаві та відрізняють ефективність, надану обома протоколами. На рисунку 4.3 видно, що у випадку 0,1% втрати пакетів поведінка SCTP залишається на контролі. Він дійсно досягає межі понад 1 секунду, але досить швидко відновляється після кожної аномальної події. Тоді як UDP показує затримку до 600 мс кожного разу, коли пакет падає. Хоча пікова затримка, з якою стикається SCTP, є більшою, ніж досягнута UDP, все ж SCTP є досить конкурентоспроможною, щоб її можна було розглядати як потенційного кандидата, оскільки в цілому ефективність роботи не погіршується повністю.

На рисунку 4.4 показано продуктивність протоколів при втраті 0.2% пакетів.

Тут ми бачимо, що затримка починає наростати, і максимальний ступінь затримки, досягнутий SCTP тут, становить близько 1,8 секунди, що є досить високим показником, особливо з огляду на потреби в телефонній сигналізації в реальному часі. Це випливає з того, що прикладний рівень продовжує надсилати пакети через рівні проміжки часу, але транспортний рівень утримує ці пакети в своєму буфері і не надсилає їх відразу, оскільки надсилання обмежується вікном перевантаження. Оскільки швидкість дзвінків зберігається фіксованою, тому будь-які втрачені пакети спричиняють зменшення вікна перевантаження вдвічі, що ще більше руйнує запити, оскільки окрім INVITE, повідомлення також впливає на вікно перевантажень.

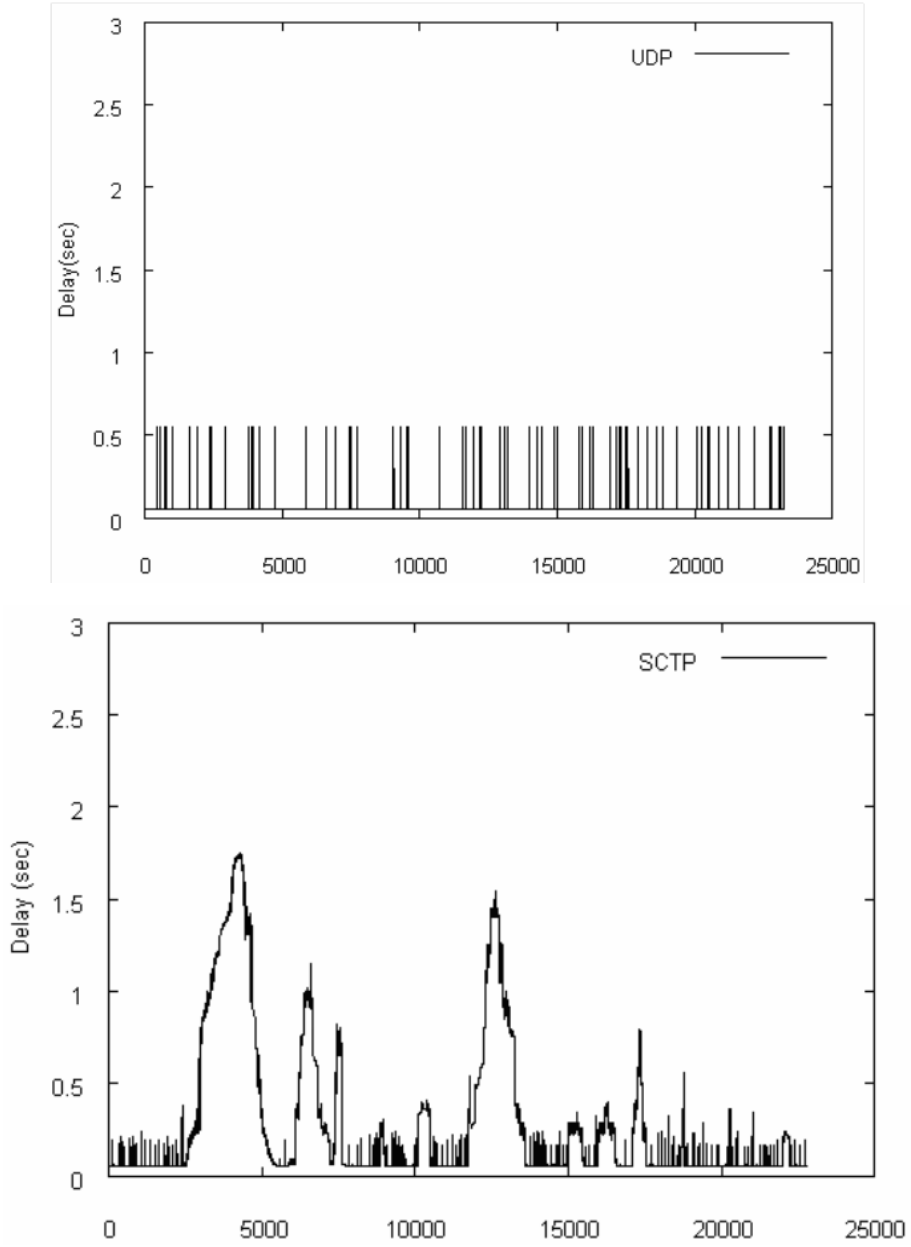
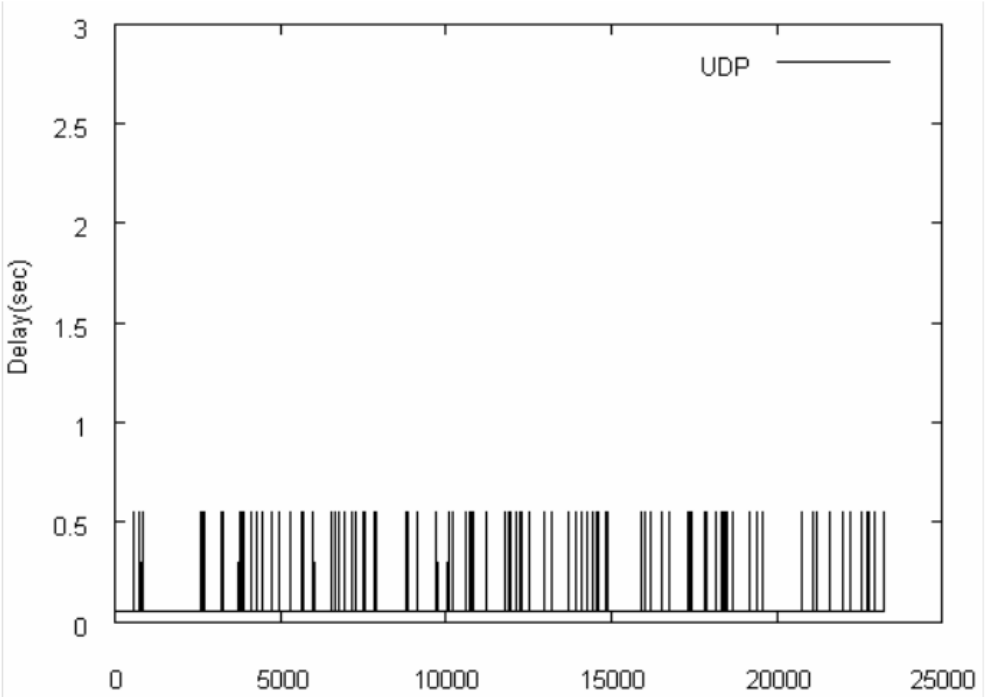


Рисунок 4.4 – Продуктивність протоколів при втраті 0.2% пакетів

У випадку UDP змінюється лише інтенсивність утворення затримок, але час затримки зберігається на тому ж рівні, що і в минулому експерименті.

Подібним чином, при коефіцієнті втрат 0,3% результати виходять за межі 2,5 секунди. Отже висновок, який можна зробити з цього дослідження втрати пакетів, полягає в тому, що SCTP не може жити, збільшуючи втрати пакетів.

На рисунку 4.5 показано продуктивність протоколів при втраті 0.3% пакетів.



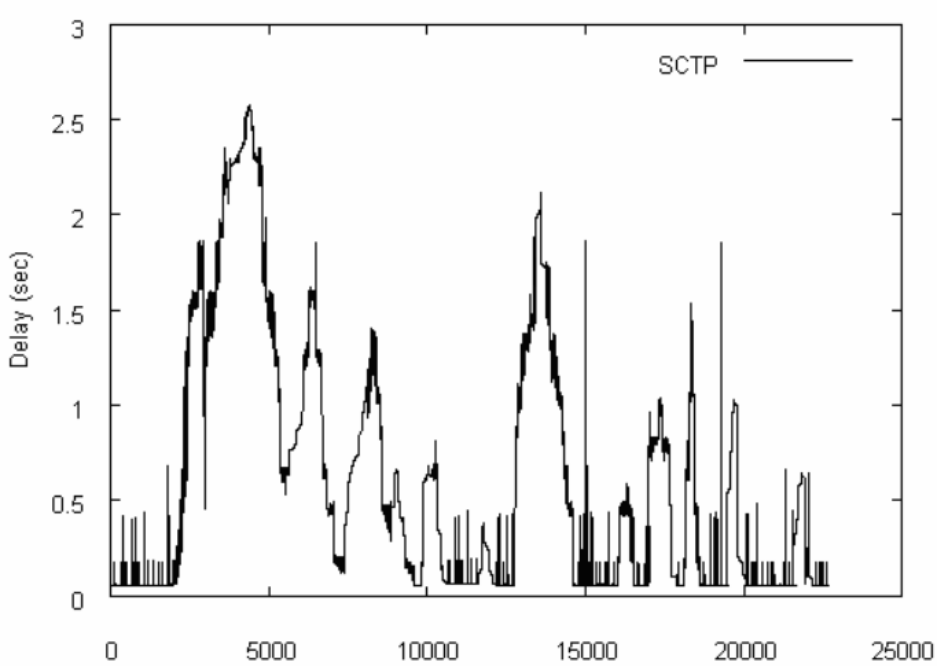


Рисунок 4.5 - Вплив випадкової втрати пакетів 0,3%

Основна відмінність тут у сценарії SIP-T та проксі-сервері SIP полягає в тому, що у проксі-сервері SIP єдиним повідомленням, надісланим від кінця відправника, є INVITE, і воно отримує попередні відповіді “ Trying” та “ Call” від одержувача, тоді як у випадку SIP-T всі повідомлення SIP щодо встановлення, управління та припинення сеансів обробляються MGC. Отже,

звичайним повідомленням в доповнення до INVITE є ACK/200OK. Втрата ACK/200OK призведе до того, що SCTP дає більші затримки через збільшення втрати пакетів, при цьому вікно перевантажень страждає все більше. Для того, щоб всі пакети вмістилися, вони скидаються на транспортний шар, при цьому це стає справжнім ударом по продуктивності.

4.2.3 Пропускна здатність

Цей експеримент призначений для пошуку пропускної здатності, досягнутої UDP та SCTP, імітуючи безперервний ефект перехресного трафіку. Трафік що генерується на вузлі 4 використовує TCP як транспортний протокол. Іншим змінним параметром, що використовується тут, є розмір буфера маршрутизатора, приєднаного до вузла 0. На наведеному нижче графіку показана пропускна здатність, досягнута SCTP та UDP з розмірами буферів 5, 20, 50, 100, 150, 200 і 250. Знову зрозуміло UDP демонструє домінування, особливо із зменшенням розміру буфера. UDP здатний надіслати майже всю необхідну кількість повідомлень у встановлений час, тоді як пропускна здатність для SCTP сильно варіюється, перебуваючи в нижній частині з меншими розмірами буфера і збільшується зі збільшенням розмірів буфера.

Показники пропускної здатсті, досягнутої за допомогою UDP і SCTP, з різними розмірами буфера, що супроводжується постійною конкуренцією за вузьке місце, показано на рисунку 4.6.

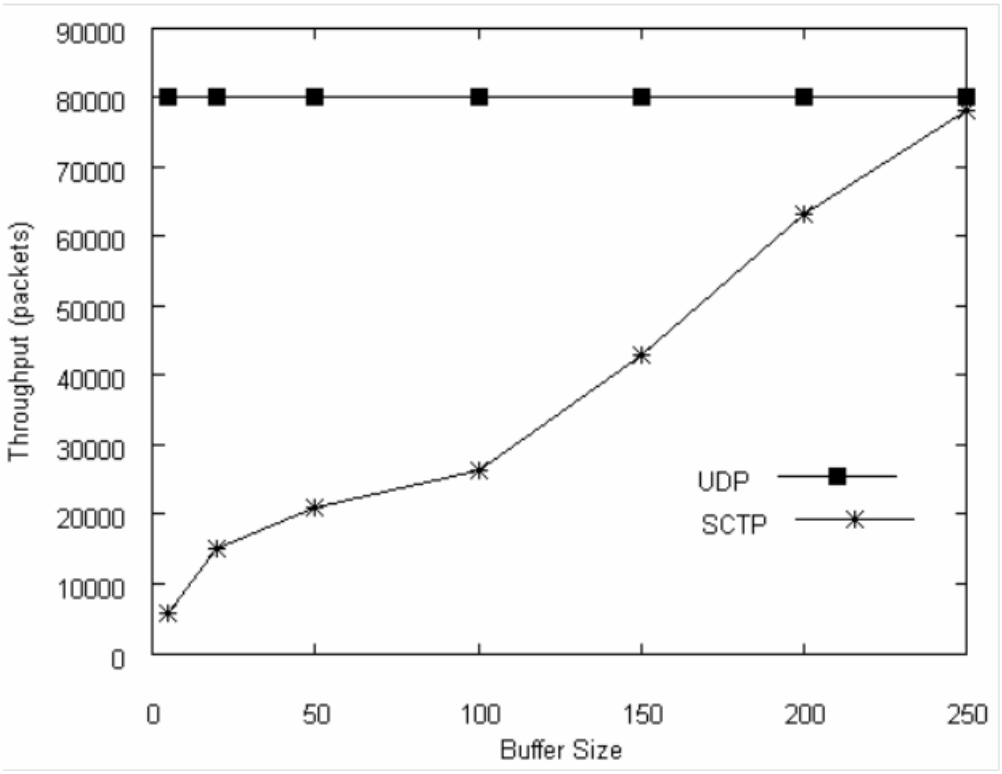


Рисунок 4.6 - Пропускна здатність, досягнута за допомогою UDP і SCTP, з різними розмірами буфера, що супроводжується постійною конкуренцією за вузьке місце

Знову ж таки видно, що UDP працює краще, і причина очевидна, бо UDP не має транспортних накладних витрат, не контролює потоки, не контролює затори, не має повільних запусків. Це працює чітко, зберігаючи справу дуже простою та прямою, хоча і не є привітним для сучасного Інтернет-трафіку з часткою TCP понад 80%.

4.3 Висновки до розділу 4

В даному розділі, в рамках дослідження взаємодії мережі SIP з мережею з інтеграцією послуг, було проведене моделювання трьох випадків транспортування повідомлень сигналізації при використанні різних типів обмежень, щоб визначити більш відповідний протокол для вирішення поставленої задачі.

Перший експеримент був зроблений для порівняння продуктивності двох протоколів із перехресним трафіком на вузькому місці. Ми спостерігали більш-менш задовільну ефективність конкуруючого трафіку з UDP і SCTP, хоча UDP має перевагу, позбавлену всіляких транспортних накладних витрат. Але у випадку втрати пакетів, де SCTP зазнає незначних змін затримки, UDP страждає від ефекту повторної передачі рівня додатків.

Другий експеримент був розроблений для моніторингу впливу втрати пакетів на продуктивність досліджуваних протоколів. Зі збільшенням ефекту втрати пакетів продуктивність SCTP зазнає серйозного погіршення. Ця деградація у випадку SIP-T (MGC) більша за величиною порівняно з випадком SIP Proxy. UDP, з іншого боку, зберігає послідовну поведінку. Однакова швидкість втрати пакетів у SCTP спричиняє падіння пакетів на транспортному рівні та послідовне збільшення затримок. Тому дуже легко помітити, що SCTP не має порівняння з UDP. Оскільки трафік Інтернету дуже бурхливий, і важко передбачити щільність і втрати трафіку, так само непросто дати чітку відповідь щодо вибору транспортного протоколу, але тип продуктивності, наданий SCTP, дає зрозуміти що SCTP не можна використовувати з упевненістю, оскільки навіть рівень втрат у 0,2% значно погіршує його продуктивність порівняно з UDP.

Аналогічним чином пропускна здатність, надана SCTP, сильно залежила від розміру буфера, і при його зменшенні значно погіршувалась продуктивність, запропоновану SCTP. З іншого боку, UDP вирізняється навіть за розміру буфера в 5 пакетів, що було чітко показано в результатах третього експерименту.

Згідно результатів дослідження, при ситуації конкуруючого трафіку обидва протоколи мають майже рівну затримку. Не зважаючи на це, за наявності невеликого розміру буфера або рівня втрат пакетів вищого за 0,1%, що можливо з великою вірогідністю при експлуатації фізичних мереж зв’язку, протокол SCTP має значно гірші показники продуктивності за протокол UDP. Отже, спираючись на дані, отримані за результатами даного дослідження,

можна зробити висновок, що при використанні протоколу SIP як основного для забезпечення сигналізації між підсистемою ISUP та мережею NGN, протокол UDP залишається найпродуктивнішим протоколом для передачі SIP-повідомлень.

ВИСНОВКИ

В ході роботи було обгрунтовано актуальність дослідження алгоритмів взаємодії протоколів ЗКС №7 і SIP в телекомунікаційних мережах на базі IMS, що полягає у необхідності визначення найвідповіднішого транспортного протоколу мережі SIP.

Розглянуті алгоритми взаємодії мережі ISDN і мережі на основі протоколу SIP під час надання мультимедійних послуг та перетворення сигнальних повідомлень ISUP і SIP.

Експериментально досліджено алгоритм взаємодії сигнальних протоколів ISUP і SIP, а саме алгоритм трансляції, за умови використання транспортних протоколів SCTP та UDP.

Протокол SCTP має низку переваг перед протоколом UDP, основні з яких є гарантована доставка повідомлень, надійна передача даних, управління накопиченням пакетів, та багатопотоковість, які, безумовно, є важливими та принциповими для взаємодії мережі ISDN і мережі SIP, і цих перевагах достатньо для надання рекомендацій щодо використання саме протоколу SCTP на заміну протоколу UDP в існуючих телекомунікаційних мережах. І в даному дослідженні було порівняно продуктивність мережі SIP при використанні протоколу UDP та за можливості його заміни на протокол SCTP.

Результатом даної дипломної роботи є експериментальне визначення оптимального транспортного протоколу. За результатами експериментального дослідження виявилося, що протокол UDP має перевагу у низці показників продуктивності мережі, і дає кращі умови функціонування алгоритму трансляції трафіку.

Хоча протокол SCTP має низку переваг перед протоколом UDP, все ж за результатами дослідження можна винести рекомендації про використання саме протоколу UDP як транспортного протоколу мережі SIP.

Отже, можна зазначити, що мета роботи досягнута в повному обсязі.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Бакланов, И. Г. NGN: принципы построения и организации / под ред. Ю. Н. Чернышова. – М.: Эко-Трендз, 2008. – 400 с.: ил.

2. Кучерявый А.Е., Гильченок Л.З., Иванов А.Ю. Пакетная сеть связи общего пользования. СПб.: Наука и Техника, 2004г. , 272 стр.

3. Гольдштейн Б.С., Гольдштейн А.Б. SOFTSWITCH – СПб.: БХВ – Санкт-Петербург, 2006.— 368 с

4. Session Initiation Protocol for Telephones (SIP-T) (електронний ресурс). Режим доступу: https://tools.ietf.org/html/rfc3372

5. Публічна телефонна мережа. Режим доступу: https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C_%D0%BE%D0%B1%D1%89%D0%B5%D0%B3%D0%BE_%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F

6. Signaling System #7, електроний ресурс habr. Режим доступу: https://habr.com/ru/post/113792/

7. CAP (CAMEL Application Part), електроний ресурс. Режим доступу: http://pro-gprs.info/tag/camel

8. ТМЗК, електронний ресурс. Режим доступу: https://dic.academic.ru/dic.nsf/ruwiki/1151162

9. SS7 поверх IP (електронний ресурс). Режим доступу: https://www.osp.ru/lan/2002/09/136531

10. СИСТЕМА ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ Ns-2 (електронний ресурс). Режим доступу: https://wl.unn.ru/materials/courses/wlnet/Lect/4_Lect_2.pdf

11. Лекції-Мультисервісні мережі зв'язку (електронний ресурс). Режим доступу: https://uadoc.zavantag.com/text/3927/index-1.html?page=12

12. Session Initiation Protocol (електронний ресурс). Режим доступу: https://znaimo.com.ua/SIP

13. Общеканальная система сигнализации N7 (ОКС-7). (електронний ресурс). Режим доступу: http://1234g.ru/2g/gsm/obshchekanalnaya-sistema-signalizatsii-n7-oks-7

14. Структура повідомлення підсистеми ISUP (електронний ресурс). Режим доступу: h http://um.co.ua/3/3-16/3-165810.html

15. Трансляция сетевых адресов (NAT) и SIP. Електронний ресурс. Режим доступу: https://wiki.sipnet.ru/index.php/%D0%A2%D1%80%D0%B0%D0%BD%D1%81%D0%BB%D1%8F%D1%86%D0%B8%D1%8F_%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D1%8B%D1%85_%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%BE%D0%B2_(NAT)_%D0%B8_SIP

16. Стеки протоколов: SIP и H.323. Електронний ресурс. Режим доступу: https://skomplekt.com/tools/4119471.html/

17. Дослідження технології IMS. Електронний ресур. Режим доступу: https://ru.knutd.edu.ua/publications/pdf/TD/2012-2/12levims.pdf

18. Конвергенція ТмЗК в Україні. Електронний ресурс. Режим доступу: https://www.znanius.com/3835.html

19. ПОДСИСТЕМА ISUP. Електронний ресурс. Режим доступу: https://www.opengl.org.ru/signalizatsiya-v-setyakh-svyazi/podsistema-isup.html

20. Гойхман В.Ю. IP-телефония и элементы NGN / В. Ю. Гойхман, А. Б. Гольдштейн, А. В. Зарубин. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. Бонч-Бруевича, 2012. – 31 с.

21. Порівняння протоколів tcp та udp. Електронний ресурс. Режим доступу: https://enterprise.netscout.com/edge/tech-tips/difference-between-tcp-and-udp

22. Difference between tcp and udp. Електронний ресурс. Режим доступу: https://www.diffen.com/difference/TCP_vs_UDP

23. TCP vs. UDP Ports. Електронний ресурс. Режим доступу: https://www.itprotoday.com/strategy/tcp-vs-udp-ports

24. https://www.vpnmentor.com/blog/tcp-vs-udp

25. https://www.howtogeek.com/190014/htg-explains-what-is-the-difference-between-tcp-and-udp

26. TCP vs UDP: Understanding the Difference. Електронний ресурс. Режим доступу: https://www.vpnmentor.com/blog/tcp-vs-udp

27. TCP/IP Ports and Protocols. Електронний ресурс. Режим доступу: http://www.pearsonitcertification.com/articles/article.aspx?p=1868080

28. Протоколы сетевого взаимодействия TCP/IP. Електронний ресурс. Режим доступу: https://www.opennet.ru/docs/RUS/tcpip/

29. Протоколы транспортного уровня (TCP, UDP, SCTP). Електронний ресурс. Режим доступу:

https://neerc.ifmo.ru/wiki/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D1%82%D1%80%D0%B0%D0%BD%D1%81%D0%BF%D0%BE%D1%80%D1%82%D0%BD%D0%BE%D0%B3%D0%BE_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D1%8F_(TCP,_UDP,_SCTP)